VERITAS NetBackup™ 3.4

Troubleshooting Guide

UNIX

June 2000
100-001518

VERITAS

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Copyright

Copyright © 1998-2000 VERITAS Software Corporation. All rights reserved. VERITAS is a registered trademark of VERITAS Software Corporation in the US and other countries. The VERITAS logo, VERITAS NetBackup, and VERITAS NetBackup BusinesServer are trademarks of VERITAS Software Corporation. All other trademarks or registered trademarks are the property of their respective owners.

Portions of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright 1991-92, RSA Data Security, Inc. Created 1991. All rights reserved.

Printed in the USA, June 2000.

VERITAS NetBackup Troubleshooting Guide - UNIX

VERITAS Software Corporation
1600 Plymouth St.
Mountain View, CA 94043
Phone 650–335–8000
Fax 650–335–8050
www.veritas.com

Contents

Preface . . . . . **ix**
Audience ix
Organization ix
Related Manuals x
Conventions x
Type Style x
Notes and Cautions x
Key Combinations xi
Command Usage xi
Getting Help xi

Chapter 1. Introduction **1**
Define the Problem 1
What was the Error Indication? 1
What Were You Trying to Do When the Problem Occurred? 1
Record All Information 2
Troubleshooting the Problem 4
Problem Report Information 5
General Information 5
Gathering Information for NetBackup-Java 6

Chapter 2. Troubleshooting Procedures **9**
Preliminary Troubleshooting 9
Troubleshooting Installation and Configuration Problems 13

To Resolve Installation Problems 13
To Resolve Common Configuration Problems 13
To Resolve Device Configuration Problems 15
General Test and Troubleshooting Procedures 18
To Test Master Server and Clients 18
Testing Media Server and Clients 21
Resolving Network Communication Problems 24
UNIX Clients 24
PC Clients 28
Verifying Host Names and Services Entries 32
Using bpclntcmd 35
Host Name and Service Entry Examples - UNIX 37
UNIX Example 1: Master Server and Client 37
UNIX Example 2: Master and Media Servers 39
UNIX Example 3: Windows, NetWare, and Macintosh Clients 41
UNIX Example 4: Clients in Multiple Networks 43
UNIX Example 5: Server Connects to Multiple Networks 44
Host Name and Service Entry Examples- Windows NT/2000 47
Windows NT/2000 Example 1: Master Server and Client 47
Windows NT/2000 Example 2: Master and Media Servers 49
Windows NT/2000 Example 3: NetWare and Macintosh Clients 51
Windows NT/2000 Example 4: Clients in Multiple Networks 53
Windows NT/2000 Example 5: Server Connects to Multiple Networks 55
Using the Configure - NetBackup Window 57

Chapter 3. Using the Logs and Reports 59

Reports 61
Status for User Operations 62
System Logs 62
Activity Logs 62

Activity Logs on Servers 62
Activity Logs on UNIX Clients 65
Activity Logs on PC Clients 66
Activity Logs on Windows and Netware Clients 66
Activity Logs on Macintosh Clients 68
Media Manager Logs 68
On UNIX 69
On Windows NT/2000 70
Windows NT/2000 Event Viewer Logging Option 70
To Enable the Logging Tool 71
eventlog File Entries 71
Example 72
Troubleshooting the Java Administration Interface 72
Enabling Detailed Activity Logging 74

Chapter 4. Status Codes and Messages 77
Status Codes 77
Messages 181

Chapter 5. Disaster Recovery 203
Master Server Disk Recovery 203
Recovering Master Server When Root is Intact 203
Recovering Master Server When Root is Lost 205
Media Server Disk Recovery 207
Client System Disk Recovery - UNIX 207
Client System Disk Recovery - Windows NT/2000, 98, 95 208
Assumptions 208
Before Starting 208
To Recover a Windows NT/2000, 98, or 95 Client Disk 209
Recommended Backup Practices 211
Recovering the NetBackup Databases 211

Identifying the Most Recent Database Backup 212
Example 1: List by Using a Raw Device 212
Example 2: List by Using a Media Manager Controlled Drive 213
Example 3: List Disk Path 213
Example 4: Media Server 214
Procedures for Recovering NetBackup Databases 214
Before Starting 215
Recover DB From Tape or Optical - Media Manager DB Lost 215
Recover DB from Tape or Optical: Media Manager DB Intact 218
Restore DB From Disk 220

Appendix A. Functional Overview 223
Backup and Restore Functional Description 223
Startup Process 224
Backup and Archive Processes 226
Backups and Archives - UNIX Clients 226
Backups and Archives - Windows 95/98 Clients 230
Backups and Archives - Windows NT/2000 Clients 231
Backups and Archives - NetWare Clients 232
Backups - Macintosh Clients 233
NetBackup Database Backups 234
Restore Processes 236
Restores - UNIX Clients 236
Restores - Windows 95/98 Clients 239
Restores - Windows NT/2000 Clients 240
Restores - NetWare Clients 241
Restores - Macintosh Clients 242
NetBackup Directories and Files 243
NetBackup Programs and Daemons 245
NetBackup Databases 254

Media Manager Functional Description 254
Startup Process 255
Media and Device Management Process 257
Barcode Operations 259
Media Requests Involving Barcodes 259
Media Manager Components 261
Media Manager Directories and Files 261
Programs and Daemons 262

Appendix B. Networks and Hostnames 271

Appendix C. Robotic Test Utilities 275
Robotic Tests on UNIX 275
Robotic Tests on Windows NT/2000 277

Glossary 279

Index 303

Preface

This guide explains how to isolate and resolve problems encountered when installing, configuring, or using VERITAS NetBackup™ for UNIX. This publication refers to VERITAS NetBackup as NetBackup.

Audience

This guide is intended primarily for the system administrator who is responsible for installing, configuring, and managing NetBackup. The system administrator is assumed to have a good working knowledge of both NetBackup and UNIX. Some sections will also be useful to less-technical users who encounter problems when backing up, archiving, or restoring files.

Organization

- Chapter 1, “Introduction,” explains how to define a problem and describes the information you should gather during troubleshooting. Both administrators and client users should read this chapter first.
- Chapter 2, “Troubleshooting Procedures,” includes procedures for isolating the problem to a specific area.
- Chapter 3, “Using the Logs and Reports,” discusses the NetBackup logs and how to interpret them.
- Chapter 4, “Status Codes and Messages,” explains each status code and provides corrective actions for error conditions.
- Chapter 5, “Disaster Recovery,” explains how to recover critical NetBackup information in case of a disk crash.
- Appendix A, “Functional Overview,” provides a functional overview of NetBackup and its Media Manager component, for both Windows and UNIX.
- Appendix B, “Networks and Hostnames,” provides information useful when configuring NetBackup on a host with multiple network connections and when hosts have multiple names.

- Appendix C, "Robotic Test Utilities," explains how to start the tests that are included with the robotic software.

Following the appendixes is a glossary of NetBackup terms.

Related Manuals

Refer to the *NetBackup Release Notes* for a complete list of NetBackup manuals.

Conventions

The following explains typographical and other conventions used in this guide.

Type Style

Table 1. Typographic Conventions

Typeface	Usage
`Bold fixed width`	Input. For example, type **`cd`** to change directories.
`Fixed width`	Paths, commands, filenames, or output. For example: The default installation directory is `/opt/VRTSxx`.
Italics	Book titles, new terms, or used for emphasis. For example: *Do not* ignore cautions.
Sans serif (italics)	Placeholder text or variables. For example: Replace *filename* with the name of your file.
Sans serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the Password field.

Notes and Cautions

Note This is a Note and is used to call attention to information that makes it easier to use the product or helps you to avoid problems.

Caution This is a Caution and is used to warn you about situations that can cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, you may have to hold down the Ctrl key before you press another key. When this type of command is referenced, the keys are connected by plus signs. For example:

Press Ctrl+t

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

`command` *arg1* | *arg2*

the user can use either the *arg1* or *arg2* variable.

Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

`http://www.veritas.com/`

For product assistance, contact VERITAS Customer Support.

US and Canadian Customers: 1-800-342-0652

International Customers: +1 (650) 335-8555

VERITAS Customer Support can also be reached through electronic mail at:

`support@veritas.com`

Introduction 1

This chapter explains the basic steps to take if you encounter a problem while using NetBackup. Other chapters provide more specific information.

Note The term *media server*, as distinct from *master server* or *server*, does not apply to the NetBackup BusinesServer product. When troubleshooting a BusinesServer installation, please ignore any references to media server in this guide.

Define the Problem

The first step in troubleshooting is to define the problem.

What was the Error Indication?

In defining the problem, you must know what went wrong and sometimes resolving the problem also requires that you also know what went right.

Error messages are usually the vehicle for telling you something went wrong. So the first thing to do is look for an error message. If you don't see an error message in an interface, but still suspect a problem, check the reports and logs. NetBackup provides extensive reporting and logging facilities and these can provide an error message that points you directly to a solution.

The logs also show you what went right and what NetBackup was doing when the problem occurred. For example, a restore can be waiting for media to be mounted and the required media is currently in use for another backup.

Chapter 3 describes the log information that NetBackup provides. Chapter 4 provides interpretations of NetBackup status codes and messages.

What Were You Trying to Do When the Problem Occurred?

Another important part of defining the problem is to clearly define what you were trying to do in the first place.

Some questions to ask here are:

- What operation was being attempted?
- What method were you using? For example, there is more than one way to install software on a client. There is also more than one possible interface to use for many operations and some operations can even be performed with a script.
- What type of server platform and operating system was involved?
- If your site uses both master and media servers, was it a master or a media server?
- If a client was involved, what type of client was it?
- Have you ever performed the operation successfully in the past? If so, what is different now?
- What is the service pack level?

Record All Information

As you define and troubleshoot a problem, always try to capture potentially valuable information, such as:

- NetBackup progress logs
- NetBackup Reports
- NetBackup activity logs
- Media Manager debug logs
- On UNIX NetBackup servers, check for error or status messages in the system log or standard output
- Error or status messages in dialogs
- On Windows NT/2000 NetBackup servers, check for error or status information in the Event Viewer Application log

Record this information for each attempt. A benefit of this approach is that you can compare the results of multiple attempts. It is also useful for others at your site and for customer support in the event that you cannot solve the problem yourself.

Chapter 3 explains the various logs.

If your troubleshooting attempt is unsuccessful, customer support can provide further assistance. Before calling, have the following information ready.

- Product, platform, and device information:
  - Product and its release level.
  - Server hardware type and operating system level.

- Client hardware type and operating system level, if a client is involved.
- Storage units being used, if it is possible that storage units are involved.
- If it looks like a device problem, be ready to supply device information, such as the types of robots and drives along with Media Manager and system configuration information.
- Software patches to the products that were installed.
- Service packs and hotfixes that were installed (Windows NT/2000).

- What is the definition of the problem as described earlier in this chapter? Copies of logs or core dumps (if any) can also be required.
- Have you had this problem before? If so, was there a successful resolution and what did you try that time?
- Has the configuration been changed recently and, if so, what was changed?
- If necessary, can you communicate with technical support through `ftp`, email, or fax? This can be useful for sending things such as copies of logs.

"Problem Report Information" on page 5 lists the information you need and also provides methods for gathering information.

Troubleshooting the Problem

After defining the problem, use the information in the other chapters of this manual to try and correct it.

- When you have a status code or message, proceed directly to Chapter 4 and try the corrective actions recommended there.
- When you do not see a status code or message, or the actions in Chapter 4 do not solve the problem, try the troubleshooting procedures in Chapter 2. Those procedures describe an effective approach for isolating common problems.

If you don't find the solution, obtain assistance by contacting customer support.

Problem Report Information

General Information

Date: _____

Servers (master and media):

Platform Types and Host Names	OS Levels	Product Version and Patch Levels

Clients:

Platform Types and Host Names	OS Levels	Product Version and Patch Levels

What were you attempting when the problem occurred? (for example, a backup on a Windows NT/2000 client)

_____

_____

What were the error indications? (for example, status code, error dialog box)

_____

_____

_____

Did this occur during or shortly after any of the following:

_____ Initial Installation

_____ Configuration change (explain)

_____ System change or problem (explain)

_____ Have you seen the problem before: (if so, what did you do that time)

Logs or other failure data you have saved:

_____ All log entries report

_____ Media Manager debug logs

_____ NetBackup activity logs

_____ System logs (UNIX)

_____ Event Viewer Application logs (Windows NT/2000)

Can you communicate with us through any of the following:

_____ ftp

_____ telnet

_____ email

_____ fax

Gathering Information for NetBackup-Java

If you encounter problems with the NetBackup-Java applications, use the following methods to gather data for VERITAS support.

The following scripts are available for gathering information:

- The NetBackup-Java administration application startup script, `jnbSA`, logs data to a log file in `/usr/openv/java/logs`. At startup, the script tells you which file in this directory it is logging to. Normally, this file does not become very large (usually less than 2 KB). Changing the `debugLevel` option in the `Launch.properties` file is a way to get more data written to the log file. However, do not change this option without consulting VERITAS customer support.
- The `/usr/openv/java/get_trace` script provides a Java virtual machine stack trace for support to analyze. This stack trace is written to the log file associated with the instance of execution (see previous bullet).
- The `/usr/openv/netbackup/bin/goodies/support` script creates a file containing data necessary for customer support to debug any problems you encounter. For more details, consult the usage information of the script by using `support -h`.

Follow these steps to get debug data for VERITAS support to analyze:

1. If the application does not respond for a long time, it may be hung. However, some operations can take quite a while to complete. This is especially true in the Activity Monitor and Reports applications. So, wait for several minutes before assuming the operation is hung.

   If there is no response within several minutes, execute `/usr/openv/java/get_trace` under the account where you started the Java application. This causes a stack trace to be written to the log file.

   For example, if you started `jnbSA` from the root account, start `/usr/openv/java/get_trace` as root. Otherwise, the command executes without error, but fails to add the stack trace to the debug log. This occurs because root is the only account that has permission to execute the command that dumps the stack trace.

2. Execute `/usr/openv/netbackup/bin/goodies/support` to get data about your configuration. Execute this script after completing NetBackup installation and each time after you change the NetBackup configuration.

3. Provide the support-script output and log file to VERITAS support.

Troubleshooting Procedures 2

This chapter has procedures for finding the cause of NetBackup errors. These procedures are general in nature and do not attempt to cover every problem that could occur. They do, however, recommend methods that usually result in successful problem resolution.

When performing these procedures, try each step in sequence. If you have already performed the action or it does not apply, skip to the next step. If it branches you to another chapter, use the solutions suggested there. If you still have a problem, go to the next step in the procedure. Also, alter your approach based on your specific configuration and what you have already tried.

There are three troubleshooting procedures:

- Preliminary Troubleshooting
- Troubleshooting Installation and Configuration Problems
- General Test and Troubleshooting Procedures

Start with "Preliminary Troubleshooting." This explains what to check first and then branches off to other procedures as appropriate. "Troubleshooting Installation and Configuration Problems" applies specifically to installation and configuration problems. "General Test and Troubleshooting Procedures" defines general methods for finding server and client problems and should be used last.

Note The term *media server*, as distinct from *master server* or *server*, does not apply to the NetBackup BusinesServer product. When troubleshooting a BusinesServer installation, please ignore any references to media server.

Preliminary Troubleshooting

If you are having problems with NetBackup, perform this procedure first.

1. Ensure that your servers and clients are running supported operating system versions and the peripherals you are using (if any) are supported. See the NetBackup release notes for this information.

2. Check for status codes or messages.

a. Use the All Log Entries report and check for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred and can often provide specific information that is useful when the status code can result from a variety of problems.

If the problem involved a backup or archive, check the Backup Status report. This report gives you the status code.

If you find a status code or message in either of the above reports, go to Chapter 4 and perform the recommended corrective actions.

b. If the problem pertains to media or device management and either NetBackup does not provide a status code or you cannot correct the problem by following the instructions in Chapter 4, check the system log (UNIX) or Event Viewer Application log (Windows NT/2000). This log can show the context in which the error occurred and the error messages are usually descriptive enough to point you to a problem area.

c. Check applicable activity or debug logs that are enabled and correct problems you detect.

If these logs are not enabled, enable them before retrying the failed operation (see Chapter 3).

d. If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to step 3 below.

3. If you encountered the problem:

- During a new installation
- During an upgrade installation
- After making changes to an existing configuration

Then, go to "Troubleshooting Installation and Configuration Problems" on page 13.

4. Ensure that the server and client are operational.

If the server or client disk crashed, refer to Chapter 5 for procedures on recovering files that are critical to NetBackup operation.

Verify there is enough space available in the disk partitions that NetBackup uses. If one or more of these partitions is full, NetBackup processes that access the full partition will fail. The resulting error message depends on the process but you could see messages such as "unable to access" or "unable to create or open a file."

Check the following disk partitions:

- The partition where NetBackup software is installed.

- On the NetBackup master or media server, the partition where the NetBackup (or Media Manager) databases reside.
- The partition where the NetBackup processes write temporary files.
- The partition where NetBackup logs are stored.
- The partition where the operating system is installed.

On UNIX, use the `df` command to view disk partition information. On Windows NT/2000, use Disk Manager or Explorer.

5. Enable verbose logging either for everything or just for areas you think are related to the problem. See Chapter 3 for information on verbose logging.

6. On UNIX NetBackup servers, determine which daemons and processes are running by executing:

   ```
   /usr/openv/netbackup/bin/bpps -a
   ```

   a. If either the NetBackup request daemon (`bprd`) or database manager daemon (`bpdbm`) are not running, execute this command to start them:

   ```
   /usr/openv/netbackup/bin/initbprd
   ```

   b. If any of the following media and device management processes are not running:

   - `ltid` (device)
   - `vmd` (volume)
   - `avrd` (automatic volume recognition)
   - processes for all configured robots

   stop the device daemon, `ltid`, by executing:

   ```
   /usr/openv/volmgr/bin/stopltid
   ```

   Stop any robot control daemons that remain running when `ltid` is terminated. Then, start all daemons by executing:

   ```
   /usr/openv/volmgr/bin/ltid
   ```

   For debugging, it is best to start `ltid` with the `-v` (verbose) option.

7. On Windows NT/2000 NetBackup servers, verify that the required services and processes are running:

a. Use the NetBackup Activity Monitor, or the Services application in the Windows NT/2000 Control Panel, to start the following services if they are not running:

Note To start all of them, execute *install_path*\NetBackup\bin\bpup.cmd.

On NetBackup master servers:

- NetBackup Request Manager service
- NetBackup Database Manager service
- NetBackup Device Manager service (if the system has devices configured)
- NetBackup Volume Manager service
- NetBackup Client service

On NetBackup media servers:

- NetBackup Device Manager service (if the system has devices configured)
- NetBackup Volume Manager service
- NetBackup Client service

On NetBackup clients (including administration clients)

- NetBackup Client service

b. Use the NetBackup Activity Monitor to see if the following Media Manager processes are running:

- `avrd` (automatic volume recognition)
- Processes for all configured robots (see the *Media Manager System Administrator's Guide - Windows NT/2000*)

If the above processes are not running, stop and then restart the NetBackup Device Manager service by using the NetBackup Activity Monitor or the Services application in the Windows NT/2000 Control Panel.

8. If you had to start any of the processes in the previous steps, retry the operation. If they are running or the problem persists, go to "General Test and Troubleshooting Procedures" on page 18.

If you cannot start any of these processes , check the appropriate activity logs (see Chapter 3) for NetBackup problems.

When started, these processes continue to run unless you stop them manually or there is a problem with the system. It is best to add commands for starting them your startup scripts, so they are restarted in case you have to reboot.

Troubleshooting Installation and Configuration Problems

To Resolve Installation Problems

1. Could you install the software on the master and media servers by using the release media?

   Some reasons for failure could be:

   - Permission denied (ensure you have permission to use the device and to write the directories and files being installed)
   - Bad media (contact customer support)
   - Defective drive (replace the drive or refer to vendor's hardware documentation)
   - Improperly configured drive (refer to system and vendor documentation)

2. Could you install NetBackup client software on the clients?

Note You cannot install PC client software from a UNIX NetBackup server.

   - For an install to a trusting UNIX client, verify that you have the correct client name in your class configuration and the correct server name in the client `/.rhosts` file.

     If the install hangs, check for problems with the shell or environment variables for the root user on the client. The files to check depend on the platform, operating system, and shell you are using. An example for a Sun system would be if your `.login` executes an `stty` (such as `stty ^erase`) before defining your terminal type. If this caused the install process to hang, you could modify the `.login` file to define the terminal before executing the `stty` or you could move the client `.login` to another file until the install is complete.

   - For an install to a secure UNIX client, check your `ftp` configuration. For example, you must be using a user name and password that the client considers valid.

3. For general network communications problems, go to "Resolving Network Communication Problems" on page 24.

To Resolve Common Configuration Problems

If this is an initial installation or if you have changed the configuration, check for these problems before proceeding:

1. Check for the following device configuration problems:
   - Configuration for robotic drive does not specify the robot.
   - Drive is configured as wrong type or density.
   - Incorrect Robotic Drive Number.
   - SCSI ID for the robotic control is specified instead of the logical Robot Number assigned to the robot.
   - The same robot number is used for different robots.
   - SCSI ID for the drive is specified instead of a unique Drive Index number.
   - A platform does not support a device or was not configured to recognize it.
   - Robotic device is not configured to use LUN 1, which is required by some robot hardware.
   - On UNIX, drive no-rewind device path is specified as a rewind path.
   - On UNIX, tape devices are not configured with "Berkeley style close."

     This is configurable on some platforms and is required by NetBackup (see the *Media Manager Device Configuration Guide* for more information).
   - On UNIX, tape devices (other than QIC) are not configured as "variable mode." This is configurable on some platforms and is required by NetBackup.

     When this condition exists, you can frequently perform backups but not restores. "Status Code: 174" on page 144 provides further explanation. Also see the *Media Manager Device Configuration Guide*.
2. Check for the following problems with the daemons:
   - Daemons do not start during reboot (configure system so this occurs).
   - Wrong daemons are started (problems with media server start up scripts).
   - Configuration was changed while daemons were running.
   - On Windows NT/2000, the `%SystemRoot%\System32\drivers\etc\services` file does not have an entry for `vmd`, `bprd`, `bpdbm` and `bpcd`. Also, ensure there are entries for the processes for configured robots (see the *Media Manager System Administrator's Guide - Windows NT/2000* for a list of these processes).
   - On UNIX, the `/etc/services` file (or NIS or DNS) does not have an entry for `vmd`, `bprd`, `bpdbm`, or robotic daemons.
3. If you found and corrected any configuration problems, retry the operation and check for NetBackup status codes or messages.

a. Check the All Log Entries report for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred and can often have specific information that is useful when the error can result from a variety of problems.

If the problem involved a backup or archive, check the Backup Status report. This report gives you the status code.

If you find a status code or message in either the Backup Status or All Log Entries report, go to Chapter 4 and perform the recommended corrective actions.

b. If the problem pertains to device or media management and either NetBackup does not provide a status code or you cannot correct the problem by following the instructions in Chapter 4 check the system log (Event Viewer Application log on Windows NT/2000) for NetBackup entries.

c. Check appropriate activity logs that are enabled and correct problems you detect.

If these logs are not enabled, enable them before your next attempt. For more information, see Chapter 3.

d. If you performed corrective actions as a result of step a through step c, retry the operation. If you did not perform corrective actions or the problem persists, go to the next section, "General Test and Troubleshooting Procedures."

To Resolve Device Configuration Problems

Certain auto-configuration warning messages are displayed in the second panel of the Device Configuration wizard if the selected device meets any of the following conditions:

- Not licensed for NetBackup BusinesServer
- Exceeds a license restriction
- Has inherent qualities that make it difficult to auto-configure

These are the messages relating to device configuration, along with explanations and recommended actions:

Message: Drive does not support serialization

Explanation: The drive does not return its serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration will not function optimally, the drive can be operated without its serial number.

Recommended Action: Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or operate the drive without a serial number.

Message: Robot does not support serialization

Explanation: The robot does not return its serial number or the serial numbers of the drives contained within it. Note that some manufacturers do not support serial numbers. Although automatic device configuration will not function optimally, the robot and/or drives can be operated without serial numbers.

Recommended Action: Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or operate the robot and/or drives without serial numbers.

Message: Too many drives in robot

Explanation: The robotic library has more than two installed drives—the maximum allowed with a NetBackup BusinesServer license.

Recommended Action: Remove all but two drives.

Message: Too many slots in robot

Explanation: The robotic library has more than 22 installed slots—the maximum allowed with a NetBackup BusinesServer license.

Recommended Action: If possible, configure the robotic library to have 22 or fewer slots.

Message: No license for this robot type

Explanation: The robotic type defined for this robot is not supported by NetBackup BusinesServer.

Recommended Action: Define a different robot.

Message: No license for this drive type

Explanation: The drive type defined for this drive is not supported by NetBackup BusinesServer.

Recommended Action: Define a different drive.

Message: Unable to determine robot type

Explanation: The robotic library is not recognized by NetBackup BusinesServer. The robotic library cannot be auto-configured.

Recommended Action: Configure the robotic library manually.

Message: Drive is standalone or in unknown robot

Explanation: Either the drive or robot is not returning a serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration will not function optimally, the drive or robot can be operated without a serial number.

Recommended Action: Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or operate the drive/robot without serial numbers.

Message: Robot drive number is unknown

Explanation: Either the drive or robot is not returning a serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration will not function optimally, the drive or robot can be operated without a serial number.

Recommended Action: Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or operate the drive/robot without serial numbers.

Message: Drive exceeds drive limit

Explanation: The NetBackup BusinesServer license allows a maximum of two drives and two drives have already been configured.

Recommended Action: To use this drive, a previously configured drive must be disabled.

Message: Robot exceeds robot limit

Explanation: A robotic library has already been configured.

Recommended Action: To use this robot, a previously configured robot must be disabled.

Message: Drive is in an unlicensed robot

Explanation: The drive is in a robotic library that cannot be licensed for the NetBackup BusinesServer. Since the robot cannot be licensed for NetBackup BusinesServer, any drives configured in that robot are unusable.

Recommended Action: Configure a drive that does not reside in the unlicensed robot.

Message: Drive's scsi adapter does not support pass-thru (or pass-thru path does not exist)

Explanation: A drive was found that does not have a SCSI passthrough path configured. There are two possible causes for this message:

- The drive is connected to an adapter that does not support SCSI passthrough.
- The passthrough path for this drive has not been defined.

Recommended Action: Change the drive's adapter, or define a passthrough path for the drive.

Message: No configuration device file exists

Explanation: A device has been detected without the corresponding device file necessary to configure that device.

Recommended Action: Refer to the chapter for your system type in the *Media Manager Device Configuration Guide - UNIX* for information on creating device files.

Message: Unable to determine drive type

Explanation: The drive is not recognized by NetBackup BusinesServer. The drive cannot be auto-configured.

Recommended Action: Configure the drive manually.

General Test and Troubleshooting Procedures

If the "Preliminary Troubleshooting" or "Troubleshooting Installation and Configuration Problems" procedures did not reveal the problem, perform the following procedures, skipping those steps that you have already performed.

The procedures assume that the software was successfully installed, but not necessarily configured correctly. If NetBackup or Media Manager has never worked properly, there are probably configuration problems. Repeat the checks mentioned in the "Troubleshooting Installation and Configuration Problems" procedure when you encounter errors. In particular, look for device configuration problems.

You may also want to perform each backup and restore twice. On UNIX, perform them first as a root user and then as a nonroot user. On Windows NT/2000, perform them first as a user that is a member of the Administrators group and then as a user that is not a member of the Administrator group. In all cases, ensure that you have read and write permissions on the test files.

The explanations in these procedures assume that you are familiar with the information in Appendix A. If you have not read that appendix, do so before proceeding.

To Test Master Server and Clients

1. Enable appropriate activity and debug logs on the master server (see Chapter 3). If you do not know which logs apply, enable them all until you solve the problem. Delete the activity log directories when you have resolved the problem.

2. Configure a test class (set backup window to be open while you are testing). Name the master server as the client and a storage unit that is on the master server (preferably a nonrobotic drive). Also, configure a volume in the NetBackup volume pool and insert the volume in the drive. If you don't label the volume by using the `bplabel` command, NetBackup automatically assigns a previously unused media ID.

3. Verify that the NetBackup daemons are running on the master server:
   - To check the daemons on a UNIX system, execute:

     ```
     /usr/openv/netbackup/bin/bpps -a
     ```

   - To check the services on a Windows NT/2000 system, use the NetBackup Activity Monitor or the Services application in the Windows NT/2000 Control Panel.

4. Start a manual backup of a class by using the manual backup option in the NetBackup administration interface. Then, restore the backup.

   This verifies:

   - NetBackup server software is functional, including all daemons, programs, and databases.
   - Media Manager can mount the media and use the drive you configured.

   If a failure occurs, first check the NetBackup All Log Entries report. For failures relating to drives or media, verify that the drive is in an UP state and the hardware is functioning.

   To further isolate the problem, use the activity and debug logs. Appendix A explains the basic sequence of events (log messages are more detailed than the information in that appendix).

   If the activity logs do not reveal the problem, check the following:

   - System logs
   - Event Viewer Application logs (Windows NT/2000)
   - `vmd` debug logs on the volume database host for the device
   - `bptm` debug logs

   See the vendor manuals for information on hardware failures.

   If you are using a robot and this is an initial configuration, verify that the robotic drive is configured correctly. In particular, verify that:

   - The same robot number is used both in the Media Manager and storage unit configurations.
   - Each robot has a unique robot number.

   On a UNIX NetBackup server, you can verify only the Media Manager part of the configuration, by using the `tpreq` command to request a media mount and then assigning the drive. If this works, the problem is probably with the class or storage unit configuration. When you are done, don't forget to `tpunmount` the media.

5. If you previously configured a nonrobotic drive and your system includes a robot, change your test class now to specify a robot. Add a volume to the robot. The volume must be in the NetBackup volume pool on the volume database host for the robot.

   Repeat this procedure starting with step 3, but this time for the robot. This verifies that Media Manager can find the volume, mount it, and use the robotic drive.

   If you have difficulties with the robot, try the test utilities described in Appendix C.

Note Do not use the Robotic Test Utilities when backups or restores are active. These utilities prevent the corresponding robotic processes from performing robotic actions, such as loading and unloading media. This can cause media mount timeouts.

6. Add a user schedule to your test class (the backup window must be open while you are testing). Use a storage unit and media that has been verified in previous steps.

7. Start a user backup and restore of a file by using the client-user interface on the master server. Monitor the progress log for the operation. If successful, this operation verifies that client software is functional on the master server.

   If a failure occurs, check the NetBackup All Log Entries report. To further isolate the problem, check the appropriate activity logs from those listed below. Chapter 3 explains which logs apply to specific client software.

Note These logs exist only if you enabled activity logging in step 1. On a UNIX system, the activity logs are in the `/usr/openv/netbackup/logs/` directory. On a Windows NT/2000 system, the activity logs are in the *install_path*`\NetBackup\logs\`directory.

- `bparchive`
- `bpbackup`
- `bpbkar`
- `bpcd`
- `bplist`
- `bprd`
- `bprestore`
- `nbwin` (Windows only)
- `bpinetd` (Windows NT/2000 only)

8. Reconfigure your test class to name a client that is located elsewhere in the network. Use a storage unit and media that has been verified in previous steps. If necessary, install the NetBackup client software.

9. Create activity log directories for the processes listed below. Chapter 3 explains which logs apply to specific client types.
   - `bprd` on the server
   - `bpcd` on the client
   - `bpbkar` on the client
   - `nbwin` on the client (Windows only)
   - `bpbackup` on the client (except Windows clients)
   - `bpinetd` (Windows NT/2000 only)

10. Perform a user backup and then a restore from the client specified in step 8.

    This verifies:
    - Communications between the client and master server
    - NetBackup software on the client

    If an error occurs, check the following:
    - All Log Entries report
    - Activity logs created in the previous step

    A likely cause for errors is a communications problem between the server and the client.

11. When the test class operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.

12. When all clients and storage units are functional, test the remaining classes and schedules that use storage units on the master server. If a scheduled backup fails, check the All Log Entries report for errors, then follow the actions suggested in Chapter 4.

Testing Media Server and Clients

If you are using media servers, verify their operation as explained in the following steps. Before proceeding, eliminate all problems on the master server by completing “To Test Master Server and Clients” on page 18.

1. Enable appropriate activity and debug logs on the servers (see Chapter 3). If you are uncertain which logs apply, enable them all until you solve the problem. Delete the activity log directories when you have resolved the problem.

2. Configure a test class with a user schedule (set the backup window to be open while you are testing).
   - Name the media server as the client and a storage unit that is on the media server (preferably a nonrobotic drive).
   - Add a volume on the volume database host for the devices in the storage unit (master server is recommended for the volume database host). Ensure the volume is in the NetBackup volume pool.
   - Insert the volume in the drive. If you do not prelabel the volume by using the `bplabel` command, NetBackup automatically assigns a previously unused media ID.

3. Verify that all NetBackup daemons are running on the master server and Media Manager daemons are running on the media server.
   - To perform this check on a UNIX system, execute:

     `/usr/openv/netbackup/bin/bpps -a`
   - To perform this check on a Windows NT/2000 system, use the Services application in the Windows NT/2000 Control Panel.

4. Perform a user backup and then a restore of a file. Perform these operations from a client that has been verified to work with the master server.

   This test verifies:
   - NetBackup media server software
   - Media Manager on the media server can mount the media and use the drive that you configured
   - Communications between the master server process `bpsched` and media server processes `bpcd` and `bpbrm`
   - Communications between media server process `bpbrm` and client processes `bpcd` and `bpbkar`

   For failures relating to drives or media, ensure that the drive is in an UP state and the hardware is functioning.

   If you suspect a communications problem between the master and media servers, check the activity logs for the involved processes. If the activity logs don't help you, check the following:
   - UNIX System log

- On a Windows NT/2000 server, the Event Viewer Application log
- `vmd` debug logs

See the vendor manuals for information on hardware failures.

If you are using a robot and this is an initial configuration, verify that the robotic drive is configured correctly. In particular, verify that:

- The same robot number is used both in the Media Manager and storage unit configurations.
- Each robot has a unique robot number.

On a UNIX system, you can verify only the Media Manager part of the configuration, by using the `tpreq` command to request a media mount and then assign the drive. Perform these steps from the media server. If this works, then the problem is probably with the class or storage unit configuration on the media server or communications between the master and media server. When you are done, `tpunmount` the media.

5. If you previously configured a nonrobotic drive and a robot attached to your media server, change the test class to name the robot. Also, add a volume for the robot to the volume database host for the robot. Verify that the volume is in the NetBackup volume pool and in the robot.

Then, repeat this procedure starting with step 3, this time for a robot. This verifies that Media Manager can find the volume, mount it, and use the robotic drive.

If a failure occurs, check the NetBackup All Log Entries report. Look for errors relating to devices or media. If the All Log Entries report doesn't help, check:

- UNIX system logs on the media server
- `vmd` debug logs on the volume database host for the robot
- On a Windows NT/2000 system, the Event Viewer Application log

In an initial configuration, verify that the robotic drive is configured correctly. Do not use a robot number that is already configured on another server.

Try the test utilities described in Appendix C.

Note Do not use the Robotic Test Utilities when backups or restores are active. These utilities prevent the corresponding robotic processes from performing robotic actions, such as loading and unloading media. This can cause media mount timeouts.

6. When the test class operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.

7. When all clients and storage units are working, test the remaining classes and schedules that use storage units on the media server. If a scheduled backup fails, check the All Log Entries report for errors, then follow the actions suggested in Chapter 4.

Resolving Network Communication Problems

The following procedure is for resolving communications problems, such as those associated with status codes 54, 57, and 58. There are two variations of this procedure: one for UNIX clients and another for PC clients.

Note In all cases, ensure that your network configuration is working correctly outside of NetBackup before trying to resolve NetBackup problems.

UNIX Clients

For UNIX clients, perform the following steps. Before starting this procedure, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file. Also, create a `bpcd` activity log directory on your server and clients and a `bprd` log directory on the server. During subsequent retries, the activity logs will provide detailed debug information that will be useful in analyzing the problem.

1. If this is a new or modified configuration:

   a. Check any recent modifications to ensure that they did not introduce the problem.

   b. Ensure that the client software was installed.

   c. Ensure that the client operating system is one of those supported by the client software.

   d. Check the client names, server names, and service entries in your NetBackup configuration as explained in "Verifying Host Names and Services Entries" on page 32.

      Two other checks that you can make on host names are:

      - Use the `hostname` command on the client to determine the host name that the client sends with requests to the server.
      - Check the `bprd` activity log (verbose) on the server to determine what occurred when the server received the request.

   e. Pay special attention to NIS or DNS updates that are required. Failing to properly update these services is a common source of network problems with NetBackup.

2. Verify basic network connectivity between client and server by trying to `ping` the client from the server.

   `ping` ***`clientname`***

   Where *clientname* is the name of the client as configured in the NetBackup class configuration, `/etc/hosts`, and also in NIS and DNS (if applicable).

   For example, to `ping` a client named ant:

   ```
   ping ant
   ant.nul.nul.com: 64 byte packets
   64 bytes from 199.199.199.24: icmp_seq=0. time=1. ms
   ----ant.nul.nul.com PING Statistics----
   2 packets transmitted, 2 packets received, 0% packet loss
   round-trip (ms)  min/avg/max = 1/1/1
   ```

   Also, try `ping` from the client to the server.

   If `ping` succeeds in both instances, it verifies basic connectivity between the server and client. If ping fails, you have a network problem outside of NetBackup that must be resolved before proceeding.

   Note that some forms of the `ping` command let you `ping` the `bpcd` port on the client as in:

   ```
   ping ant 13782
   ```

   or

   ```
   ping ant bpcd
   ```

3. Check that the client is listening on the correct port for connections to `bpcd` by running one of the following commands (depending on platform and operating system).

   ```
   netstat -a | grep bpcd
   netstat -a | grep 13782 (or the value specified during the install)
   rpcinfo -p | grep 13782 (or the value specified during the install)
   ```

   For example, assume the client is a Solaris system and you execute:

   ```
   netstat -a | grep 13782
   ```

   If there is no problem with the port, the results are be similar to:

   ```
   tcp 0 0  *.13782 *.* LISTEN
   ```

   The LISTEN indicates that the client is listening for connections on this port.

   If there is a problem, this line does not appear and one of the following three conditions exists:

- /etc/services (or applicable NIS file) does not have the correct bpcd entry. The correct /etc services entry is:

  ```
  bpcd  13782/tcp    bpcd
  ```

- /etc/inetd.conf (or applicable NIS or DNS file) does not have the correct bpcd entry. The correct /etc/inetd.conf entry is:

  ```
  bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
  ```

- /etc/inetd.conf was changed but was not reread. Correct this condition by executing one of the following (whichever works):

  ```
  /bin/ps -ef | grep inetd
  kill -HUP the_inetd_pid
  ```

  or

  ```
  /bin/ps -aux | grep inetd
  kill -HUP the_inetd_pid
  ```

Note On a Hewlett-Packard platform, use `inetd -c` to send a `SIGHUP` to `inetd`.

If the problem is with an AIX client, use SMIT to verify that the InetServ object class has been updated with information about the bpcd process (/etc/inetd.conf and /etc/services information).

If you modify the InetServ object class, using SMIT, the inetexp command is automatically invoked. If you edit the InetServ object class, using an ODM editor, run the inetexp command to export the InetServ object class to the /etc/inetd.conf and /etc/services files. This keeps these files in sync with the InetServ object class.

If you change the /etc/inetd.conf or /etc/services file, using SMIT, the inetimp command automatically updates the InetServ object class. If you change either file, run the `refresh -s inetd` or `kill -1 InetdPID` command to inform the inetd daemon of the changes to its configuration file.

4. telnet to bpcd on the client. If it succeeds, keep the connection until after performing step 5, then terminate it with Ctrl-c.

```
telnet clientname 13782
```

Where *clientname* is the name of the client as configured in the NetBackup class configuration, /etc/hosts, and also in NIS and DNS (if applicable).

For example,

```
telnet ant bpcd
Trying 199.999.999.24 ...
Connected to ant.nul.nul.com.
Escape character is '^]'.
```

In this example, `telnet` can establish a connection to the client ant.

- If the `telnet` succeeds, then `inetd` on the client is configured correctly and is able to pass its connection to `bpcd` and NetBackup should also be able to establish a connection.
- If `telnet` doesn't work, ensure that the `inetd.conf` file and `/etc/services` files on both the server and client have correct and matching entries. By default, these are:

  In `/etc/services`:

  ```
  bpcd  13782/tcp    bpcd
  ```

  In `/etc/inetd.conf`:

  ```
  bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
  ```

  Then, execute `kill -HUP` to reread the `/etc/inetd.conf` file as explained in step 3.

  Also, update the applicable NIS or DNS files.

  If all these files are correct and you still cannot successfully connect to the client, suspect network routing problems or a problem with the port assignment (see next step).

5. Check that the client is listening on the correct port for the `telnet` connection to `bpcd` by running one of the following commands (depending on platform and operating system).

```
netstat -a | grep bpcd
netstat -a | grep 13782 (or the value specified during the install)
rpcinfo -p | grep 13782 (or the value specified during the install)
```

For example, assume the client in step 4 is a SunOS system named ant and the `telnet` is from a NetBackup server named whale:

```
netstat -a | grep 13782
```

- If there is no problem with the port, you see:

```
tcp 0 0  ant.nul.nul.com.13782 whale.nul.nul.com.1516  ESTABLISHED
tcp 0 0  *.13782 *.* LISTEN
```

In the first line of the result, ESTABLISHED indicates that the `telnet` connection was established to `bpcd` through port 13782 on the client.

The LISTEN in the second line indicates that the client is listening for further connections on this port.

Note We suggest that you not change the port number for bpcd or other NetBackup services. Do so only if there is no alternative; and then, remember that all NetBackup servers and clients in the configuration must use this new port assignment.

- If there is a process other than bpcd using the port, try rebooting the client to clear the problem. If the problem is still not fixed, it might be necessary to change one of the service numbers (preferably for the other service). You do this by modifying the /etc/services files then sending SIGHUP signals to the inetd processes on your clients.

  ```
  /bin/ps -ef | grep inetd
  kill -HUP the_inetd_pid
  ```

  or

  ```
  /bin/ps -aux | grep inetd
  kill -HUP the_inetd_pid
  ```

Note On a Hewlett-Packard platform, use inetd -c to send a SIGHUP to inetd.

Also make applicable NIS or DNS updates.

If the problem is with an AIX client, and you make changes to /etc/inetd.conf and /etc/services information, use SMIT to verify that the InetServ object class has been updated as explained in step 4.

6. To verify basic client to master server communications, use the bpclntcmd utility. When run on a NetBackup client, the -pn and -sv options initiate inquiries to the NetBackup master server (as configured in the bp.conf file on the client). The master server then returns information to the requesting client. For more information, see "Using bpclntcmd" on page 35.

PC Clients

1. Before retrying the failed operation:
   - Increase the logging level on the client (see the user's guide for the client).
   - On the NetBackup server, create a bprd activity log directory and on the clients create a bpcd activity log.
   - On a Windows NT/2000 NetBackup server, set the Verbose level to 1 on the General tab of the properties dialog box in the Configure - NetBackup window (see "Using the Configure - NetBackup Window" on page 57).
   - On a UNIX NetBackup server, add the VERBOSE option to the bp.conf file.

2. If this is a new client, verify the client and server names in your NetBackup configuration as explained in "Verifying Host Names and Services Entries" on page 32.

3. Verify basic network connectivity between client and server by pinging from the server to the client and from the client to the server. Use the following command:

   `ping` *hostname*

   Where *hostname* is the name of the host as configured in:

   - NetBackup class configuration
   - WINS
   - DNS (if applicable).
   - `hosts` file in the system directory:

     `%SystemRoot%\system32\drivers\etc\hosts` (Windows NT/2000)

     `C:\Windows\hosts` (default on Windows 98 and 95)

   If `ping` succeeds in all instances, it verifies basic connectivity between the server and client.

   If `ping` fails, you have a network problem outside of NetBackup that must be resolved before proceeding. As a first step, verify the workstation is turned on, as this is a common source of connection problems with PC workstations.

4. On Microsoft Windows or NetWare clients, check the NetBackup Client service:

   a. Ensure that the service is active, either by checking the logs (see step b) or as follows:

      - On Windows NT/2000 clients, use the Services application in the Control Panel to verify that the NetBackup Client service is running and start it if necessary.
      - On Windows 98 or 95 clients, check the system tray on the taskbar for the NetBackup client icon. If the icon is not there, run the NetBackup Client Job Tracker program from the NetBackup Program folder or the Start menu. When the icon is present, right-click on the icon to start the NetBackup client daemon.
      - On NetWare clients, enter `load bpcd` from the NetWare server console to start the NetBackup client daemon.

   b. Check the `bpcd` activity logs for problems or errors. See Chapter 3 for instructions on enabling and using these logs.

c. Verify that the same NetBackup client Service (bpcd) port number is specified on both the NetBackup client and server (by default, 13782).

- On Microsoft Windows, check the NetBackup Client Service Port number on the Network tab in the NetBackup Configuration dialog box. To display this dialog, start the Backup, Archive, and Restore interface on the client and click Configure on the Actions menu.

  Verify that the setting on the Network tab matches the one in the services file. The services file is located in:

  %SystemRoot%\system32\drivers\etc\services (Windows NT/2000)

  C:\Windows\services (Windows 98 and 95)

  The values on the Network tab are written to the services file when the NetBackup Client service starts.

- On NetWare clients, see the BPCD setting in the openv\netback\bp.ini file.

- Or, instead of the first bullet under step c, above: On UNIX NetBackup servers, the bpcd port number is in the /etc/services file. On Windows NT/2000 NetBackup servers, see the Client Properties dialog box in the Configure - NetBackup window (see "Using the Configure - NetBackup Window" on page 57).

Correct the port number if necessary. Then, on Windows NT/2000 clients and servers, stop and restart the NetBackup Client service. On Microsoft Windows 98 or 95 and NetWare clients, stop and restart the NetBackup client daemon (bpcd).

Note Do not change NetBackup port assignments unless it is absolutely necessary in order to resolve conflicts with other applications. If you do change them, do so on all NetBackup clients and servers. These numbers must be the same throughout your NetBackup configuration.

5. Verify that the NetBackup Request Service (bprd) Port number on Microsoft Windows and NetWare clients is the same as on the server (by default, 13720).

- On Microsoft Windows clients (use the same method as in step c under step 4).
- On NetWare clients, see the BPRD setting in the openv\netback\bp.ini file.
- Or, instead of the first bullet: On UNIX NetBackup servers, the bprd port number is in the /etc/services file. On Windows NT/2000 NetBackup servers, set these numbers in the Client Properties dialog box in the Configure - NetBackup window (see "Using the Configure - NetBackup Window" on page 57).

6. On a Macintosh client, check NetBackup configuration settings as follows:

a. Ensure that `NetBackUpListen` and `NetBackupBPCD` are in the Extensions folder.

b. Check log.*mmddyy* in the `Preferences:NetBackup:Logs:inetd` folder to see if `NetBackUpListen` is running and if it reported any errors.

c. Check log.*mmddyy* in the `Preferences:NetBackup:Logs:bpcd` folder to see if `NetBackupBPCD` was started and if it reported any errors.

d. If `NetBackUpListen` or `NetBackupBPCD` are not running, try rebooting the Macintosh. If that does not work, reinstall the software.

e. Ensure that `bpcd` port number (`portnum` in the `Preferences:NetBackup:mac.conf` file) is the same as on the server (by default, 13782).

On UNIX NetBackup servers, the `bpcd` port number is in the `/etc/services` file.

On Windows NT/2000 NetBackup servers, check the NetBackup Client Service Port number on the Network tab in the NetBackup Configuration dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the server and click Configure on the Actions menu.

Also verify that the setting on the Network tab matches the one in the services file. The `services` file is located in:

```
%SystemRoot%\system32\drivers\etc\services
```

Correct the port number, if necessary, and reboot the Macintosh.

f. Verify that the NetBackup request daemon (`bprd`) port number is the same as on the server (by default, 13720).

- On the client, this is the `bprdport` setting in the `mac.conf` file, in the NetBackup folder in the Preferences folder.
- On UNIX NetBackup servers, the `bprd` port number is in the `/etc/services` file. On a Windows NT/2000 NetBackup server, check the NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the server and click Configure on the Actions menu.

g. Ensure that other values in `mac.conf` are correct and also check the `bp.conf` file. Both files are in the Netbackup folder in the Preferences folder.

If you make changes to `mac.conf` or `bp.conf`, reboot the Macintosh.

7. Verify that the `hosts` file or its equivalent contains the NetBackup server name. On UNIX and Windows clients, the `hosts` files are:
   - `%SystemRoot%\system32\drivers\etc\hosts` (Windows NT/2000)
   - `C:\Windows\hosts` (Windows 98 or 95)
   - NetWare clients: `SYS:etc\hosts`
   - `/etc/hosts` (UNIX)
8. Verify client-to-server connectability by using `ping` or its equivalent from the client (step 3 verified the server-to-client connection).
9. If the client's TCP/IP transport allows `telnet` and `ftp` from the server, try these as additional connectivity checks.
10. For a Macintosh or NetWare client, ensure that the server is not trying to connect when a backup or restore is already in progress on the client. Attempting more than one job at a time on these clients, results in a "can't connect" or similar error.
11. Use the `bpclntcmd` utility to verify basic client to master server communications. When run on a NetBackup client, the `-pn` and `-sv` options initiate inquiries to the NetBackup master server (as configured in the server list on the client). The master server then returns information to the requesting client. For more information, see "Using bpclntcmd" on page 35.
12. Verify that the client operating system is one of those supported by the client software.

Verifying Host Names and Services Entries

This procedure is useful if you encounter problems with host names or network connections and want to verify that the NetBackup configuration is correct. Several examples follow the procedure.

Note For more information on host names, refer to Appendix B in this manual and to the "Rules for Using Host Names in NetBackup" appendix in the *NetBackup System Administrator's Guide.*

1. Verify that the correct client and server host names are configured in NetBackup.
   a. On Windows NT/2000 servers, Windows clients and NetWare nontarget clients, check the General tab in the NetBackup Configuration dialog box and the Servers tab in the Specify NetBackup Machines dialog box. To display these dialog boxes,

start the Backup, Archive, and Restore interface on the client. For the General tab, click Configure on the Actions menu; for Servers tab, click Specify NetBackup Machines on the Actions menu.

- On the Servers tab, ensure that there is a server entry for the master server and each media server.

  If you add or modify `SERVER` entries on the master server, stop and restart `bprd` and `bpdbm`.

- On the General tab, verify that the client name setting is correct and matches what is in the class client list on the master server.

- On a master or media server, ensure there is a server entry for each Windows NT/2000 administrative client that can be used to administer that server.

You can also make the above changes on the appropriate tabs in the properties dialog boxes on a Windows NT/2000 NetBackup server (see "Using the Configure - NetBackup Window" on page 57).

b. On UNIX NetBackup servers and clients, and Macintosh clients, check the server and client name entries in the `bp.conf` file:

- Ensure there is a `SERVER` entry for the master server and each media server in the configuration. The master server *must* be the first name in the list.

  Remember, if you add or modify `SERVER` entries on the master server, you must stop and restart `bprd` and `bpdbm` before the changes take effect.

- Ensure that the `CLIENT_NAME` option (if included) is correct and matches what is in the class client list on the master server.

The `bp.conf` file is in the `/usr/openv/netbackup` directory on UNIX clients and it is in the `Preferences:NetBackup` folder on Macintosh clients.

Users on UNIX clients can also have a personal `bp.conf` file in their home directory. A `CLIENT_NAME` option in `$HOME/bp.conf` overrides the one in `/usr/openv/netbackup/bp.conf`.

c. On NetWare clients, check the `openv\netback\bp.ini` file to ensure that:

- There is a `SERVER` entry for the master server and each media server in the configuration. The master server must be the first name in the list.

- The `ClientName` entry and the entries in the [clients] section are correct and match what is in the class client list on the master server.

d. On the master server, verify that you have created any required

`/usr/openv/netbackup/db/altnames` files (UNIX)

install_path`\NetBackup\db\altnames` files (Windows NT/2000)

Pay particular attention to requirements for `host.xlate` file entries.

2. Verify that each server and client has the required entries for NetBackup reserved port numbers.

Note The examples following this procedure show the default port numbers. Do not change NetBackup port assignments unless it is absolutely necessary in order to resolve conflicts with other applications. If you do change them, do so on all NetBackup clients and servers. These numbers must be the same throughout your NetBackup configuration.

a. On NetBackup servers, check the `services` files to ensure that they have entries for:

- `bpcd` and `bprd`
- `vmd`
- `bpdbm`
- Processes for configured robots (for example, `tl8cd`). See the *Media Manager System Administrator's Guide - UNIX*for a list of these processes.

On UNIX, the services file is `/etc/services`. On Windows NT/2000, the `services` file is `%SystemRoot%\system32\drivers\etc\services`.

b. On UNIX, Windows, and NetWare clients, verify the NetBackup client daemon and request daemon port numbers.

- On UNIX clients, check the `bprd` and `bpcd` entries in the `/etc/services` file.
- On Microsoft Windows clients, verify that the NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog box match the settings in the services file. To display this dialog, start the Backup, Archive, and Restore interface on the client and click Configure on the Actions menu.

  The values on the Network tab are written to the `services` file when the NetBackup Client service starts.

  The `services` file is located in:

  `%SystemRoot%\system32\drivers\etc\services` (Windows NT/2000)

  `C:\Windows\services` (Windows 98 and 95)
- On NetWare clients, check the `BPCD` and `BPRD` entries in the `openv\netback\bp.ini` file.

c. On Macintosh clients, check the `mac.conf` file in the NetBackup folder in the Preferences folder to ensure that it has the correct `portnum` and `bprdport` entries.

3. On UNIX servers and clients, check the `/etc/inetd.conf` file to ensure that it has the following entry:

```
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
```

4. On Windows NT/2000 servers and clients, verify that the NetBackup Client service is running.

5. If you are using NIS in your network, update those services to include the NetBackup information that is added to the `/etc/services` file.

6. NIS, WINS, or DNS host name information must correspond to what is in the class configuration and the name entries in the following:

- On Windows NT/2000 NetBackup servers, Microsoft Windows clients, and NetWare nontarget clients, check the General tab in the NetBackup Configuration dialog box and the Servers tab in the Specify NetBackup Machines dialog box. To display these dialog boxes, start the Backup, Archive, and Restore interface on the client. For the General tab, click Configure on the Actions menu; for Servers tab, click Specify NetBackup Machines on the Actions menu.
- The `bp.conf` file on UNIX servers and clients and Macintosh clients.
- The `openv\netback\bp.ini` file on NetWare clients.

Also, verify that reverse DNS addressing is configured.

7. To confirm the setup of the IP addresses and hostnames in DNS, NIS, and (or) local hosts files on each NetBackup node, use the NetBackup `bpclntcmd` utility.

Using bpclntcmd

The `bpclntcmd` utility resolves IP addresses into host names and host names into IP addresses by using the same system calls as the NetBackup application software. The command that starts the utility is located in the following directory:

install_path`\NetBackup\bin` (Windows NT/2000)

`/usr/openv/netbackup/bin` (UNIX)

On Windows NT/2000, run this command in an MS-DOS command window so you can see the results.

bpclntcmd options that are useful for testing the functionality of the host name and IP address resolution are -ip, -hn, -sv and -pn. The following topics explain each of these options:

bpclntcmd -ip *IP_Address*

The -ip option allows you to specify an IP address. bpclntcmd uses gethostbyaddr() on the NetBackup node and gethostbyaddr() returns the host name with the IP address as defined in the node's DNS, WINS, NIS, or local hosts file entries. No connection is established with the NetBackup server.

bpclntcmd -hn *Hostname*

The -hn option allows you to specify a host name. bpclntcmd uses gethostbyname() on the NetBackup node to obtain the IP address associated with the host name defined in the node's DNS, WINS, NIS, or local hosts file entries. No connection is established with the NetBackup server.

You can use the -ip and -hn options to verify the ability of a NetBackup node to resolve the IP addresses and host names of other NetBackup nodes. For example, you can verify that a NetBackup server can connect to a client. In this case, the steps are:

1. On the NetBackup server, use bpclntcmd -hn to verify that the operating system can resolve the host name of the NetBackup client (as configured in the client list for the class) to an IP address. The IP address is then used in the node's routing tables to route a network message from the NetBackup server.

2. On the NetBackup client, use bpclntcmd -ip to verify that the operating system can resolve the IP address of the NetBackup server (the IP address is in the message that arrives at the client's network interface).

bpclntcmd -pn

When run on a NetBackup client, the -pn option initiates an inquiry to the NetBackup master server, and the server then returns information to the requesting client. First, bpclntcmd identifies the server to which it is making the request, then it displays the information that the server returns.

For example:

```
bpclntcmd -pn
expecting response from server rabbit.friendlyanimals.com
dove.friendlyanimals.com dove 123.145.167.3 57141
```

Where:

- `expecting response from server rabbit.friendlyanimals.com` is the master server entry from the server list on the client.
- `dove.friendlyanimals.com` is the connection name (peername) returned by the master server. The master server obtained this name through `gethostbyaddress()`.
- `dove` is the client name configured in the NetBackup class client list.
- `123.145.167.3` is the IP address of the client connection at the master server.
- `57141` is the port number of the connection on the client.

`bpclntcmd -sv`

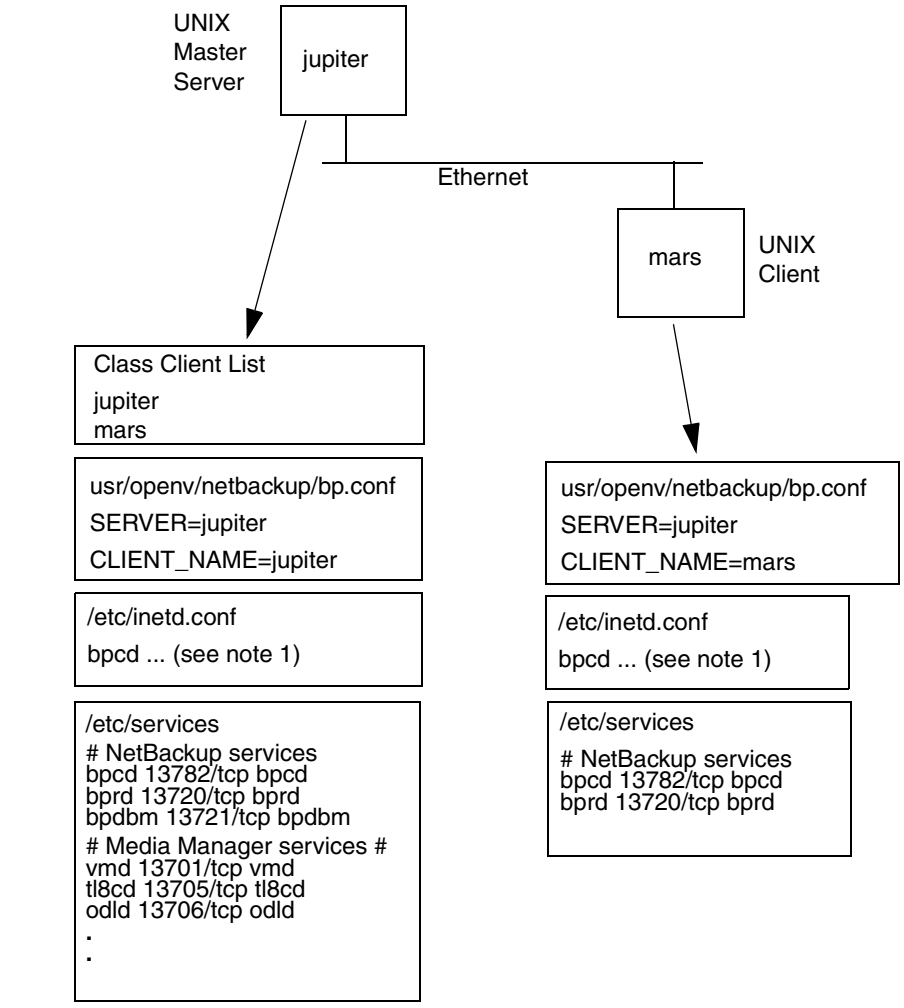
The `-sv` option displays the NetBackup version number on the master server.

Host Name and Service Entry Examples - UNIX

UNIX Example 1: Master Server and Client

The example network in the following figure shows a UNIX master server with one UNIX client.

Example 1: UNIX Master Server and Client



Notes: 1. The complete inetd.conf entry is:

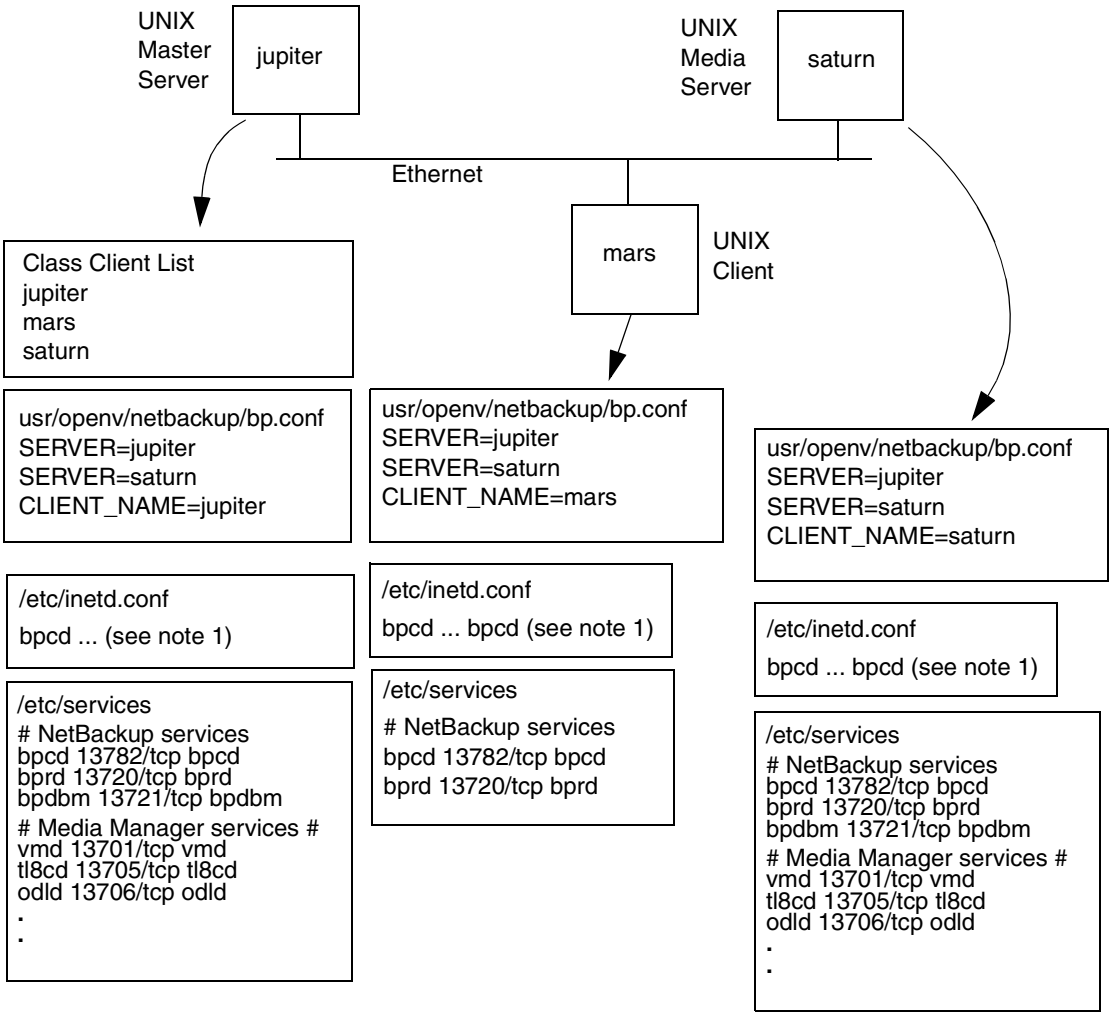
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd

2. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the /etc/hosts file and NIS, and DNS (if used).

UNIX Example 2: Master and Media Servers

The network in this example (see the next figure) is the same as the previous one except that it includes a UNIX NetBackup media server named saturn. The difference to note is the addition of a `SERVER` entry for saturn in the `bp.conf` files on all the systems. This entry is second, beneath the one for the master server jupiter.

Example 2: UNIX Master and Media Servers



Notes: 1. The complete inetd.conf entry is:

bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd

2. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the /etc/hosts file and NIS, and DNS (if used).

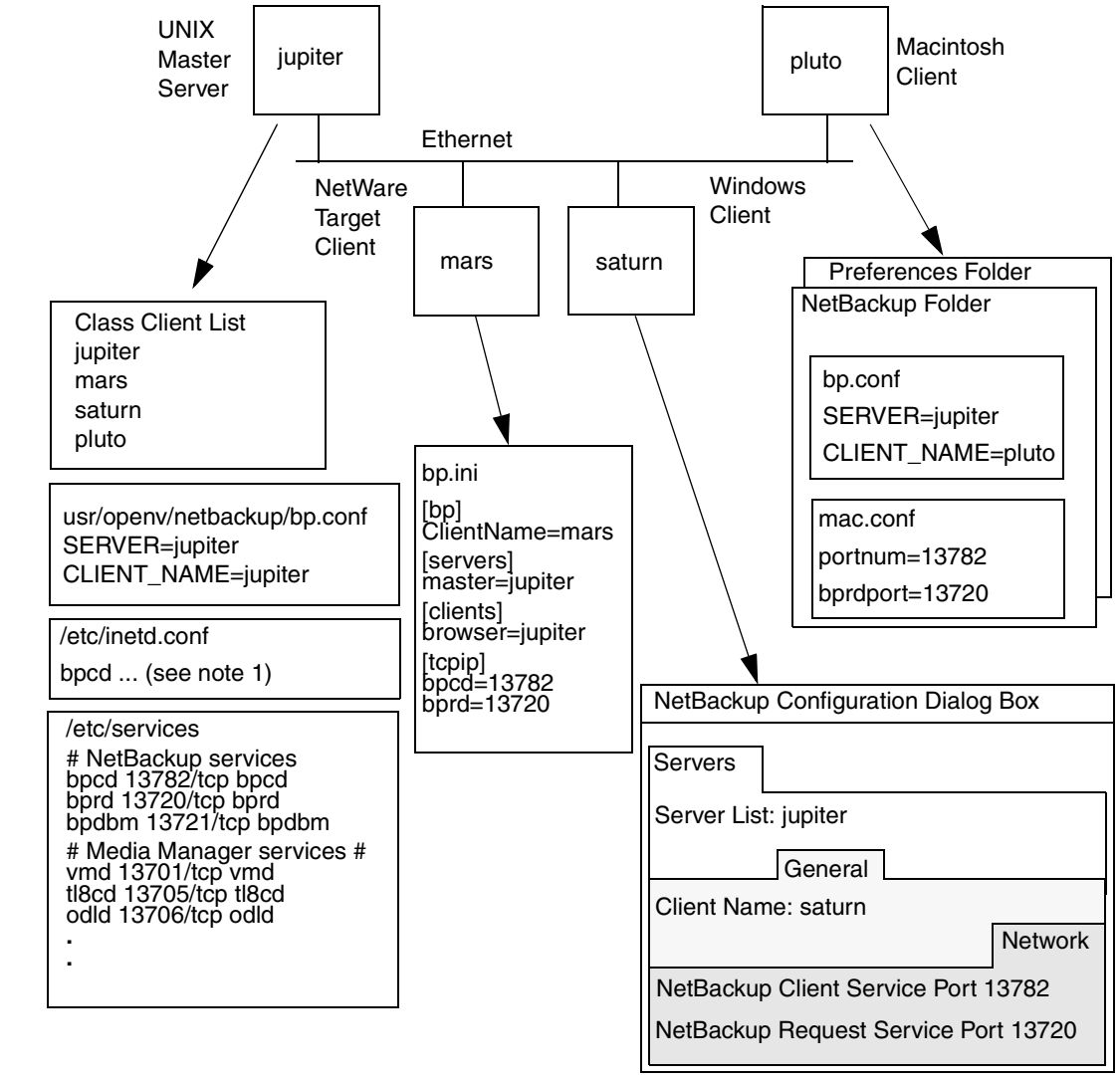
UNIX Example 3: Windows, NetWare, and Macintosh Clients

The network in this example shows a NetBackup master server with PC clients. As used here, PC client refers to Windows, NetWare, and Macintosh clients.

Note the following about this configuration:

- The configuration does not include UNIX clients but it could.
- Server configuration is the same as it is for UNIX clients.
- These specific clients do not have `inetd.conf` entries (although it is possible that some communications software includes an `inetd` equivalent).

Example 3: PC Clients



Notes: 1. The complete inetd.conf entry is:

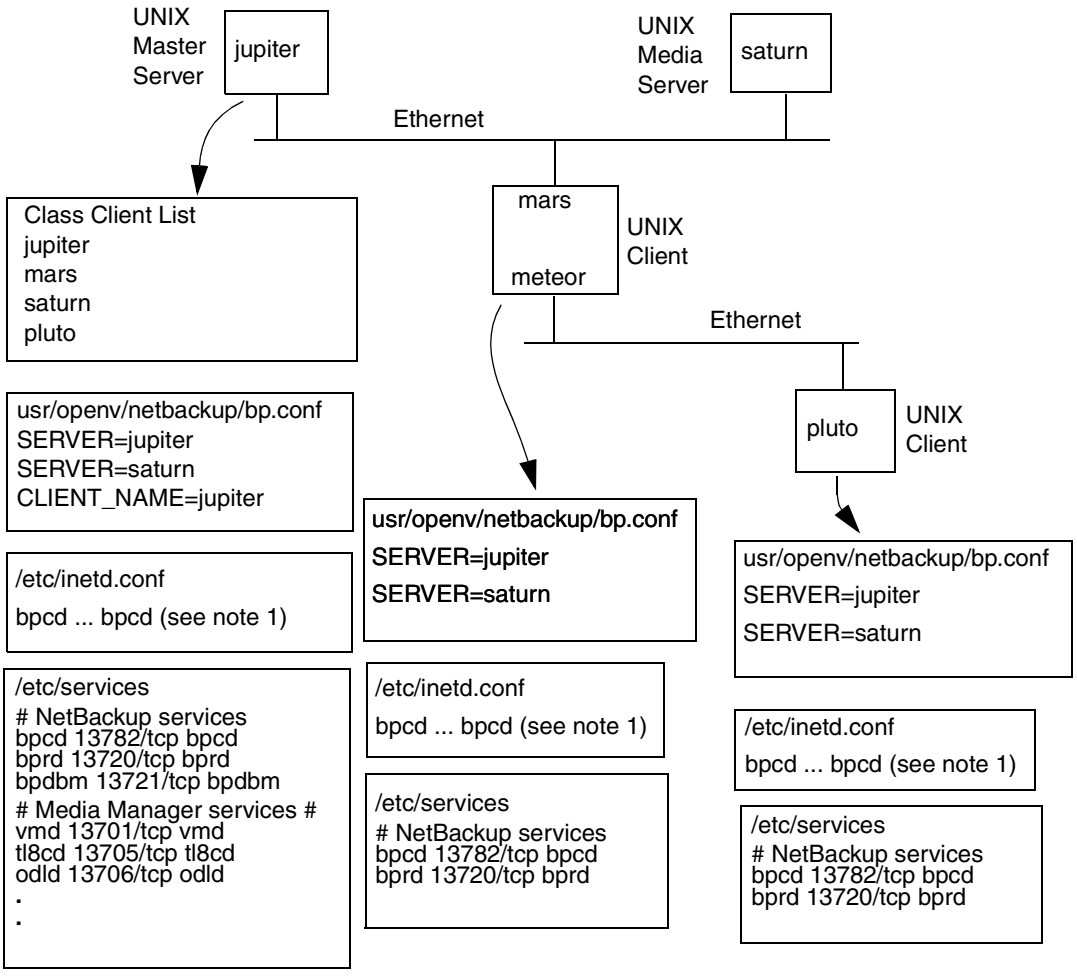
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd

2. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the /etc/hosts file and NIS, and DNS (if used).

UNIX Example 4: Clients in Multiple Networks

This network in this example (see the next figure) shows a client (mars/meteor) that is a router to clients in another network. The client's host name on the master server side is mars and the host name presented to the client pluto is meteor.

Example 4: Clients in Multiple Networks



Notes: 1. The complete inetd.conf entry is:

bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd

2. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the /etc/hosts file and NIS, and DNS (if used).

First, we examine the configuration of the router system. The NetBackup class client list shows this system as mars because that is the name of the interface to the master server. There is no special configuration to note other than the client name setting. This name must be set to mars, because this is the name that the master server recognizes.

The second client, pluto, is also configured no differently than if it were in the same network as the master server. Assuming that all the standard networking files (for example, hosts, NIS, DNS, WINS, and routing tables) are set up correctly, all the required network connections can be made.

There would be a problem, however, with restoring files from pluto if the mars/meteor system was a type of router that hides the name of the originating host when it routes requests between the two networks. For example, a router between an Ethernet and a token ring network exhibits this behavior.

To illustrate what occurs, assume that pluto is on FDDI (token ring) and the server is on Ethernet. If a user on pluto starts a restore, the router could use the name of its network interface to pluto (meteor) as the peername when it forwards the request to the server. The server interprets the request as coming from a host named meteor and does not allow the restore because meteor is not in the client list.

To resolve this problem, the administrator creates `altnames` directory on the master server and adds a file for meteor to that directory.

On a Windows NT/2000 NetBackup server, the file path is:

install_path`\netbackup\db\altnames\meteor`

On a UNIX NetBackup server, the file path is:

```
/usr/openv/netbackup/db/altnames/meteor
```

Then, the administrator adds the following line to this file:

```
pluto
```

The master server now recognizes, as legitimate, any restore requests that show a peername of meteor and client name of pluto. Refer to the *NetBackup System Administrator's Guide - UNIX* for more information on `altnames` configuration.

Regardless of the type of router, the configuration for the media server, saturn, is the same as in example 2. If a media server is involved in a backup or restore for pluto, the master server provides the correct peername and client name for the media server to use in establishing connections.

UNIX Example 5: Server Connects to Multiple Networks

The network in this example (see the next figure) shows a NetBackup server (jupter/meteor) that has two Ethernet connections and clients in both networks. The server's hostname is mars on one network and meteor on the other.

The first thing to note about this configuration is that the NetBackup class client list specifies jupiter as the client name for the master server. The list could show either jupiter or meteor *but not both*.

Another important item to note is the configuration of the NetBackup server list.

The NetBackup server list on the master server has entries for both jupiter and meteor. The reason for both names is that when the server does a backup, it uses the name associated with the client it is backing up. For example, it uses the meteor interface when backing up pluto and the jupiter interface when backing up mars. The first server entry (master server name) is jupiter because that is the name used to back up the client on the master server.

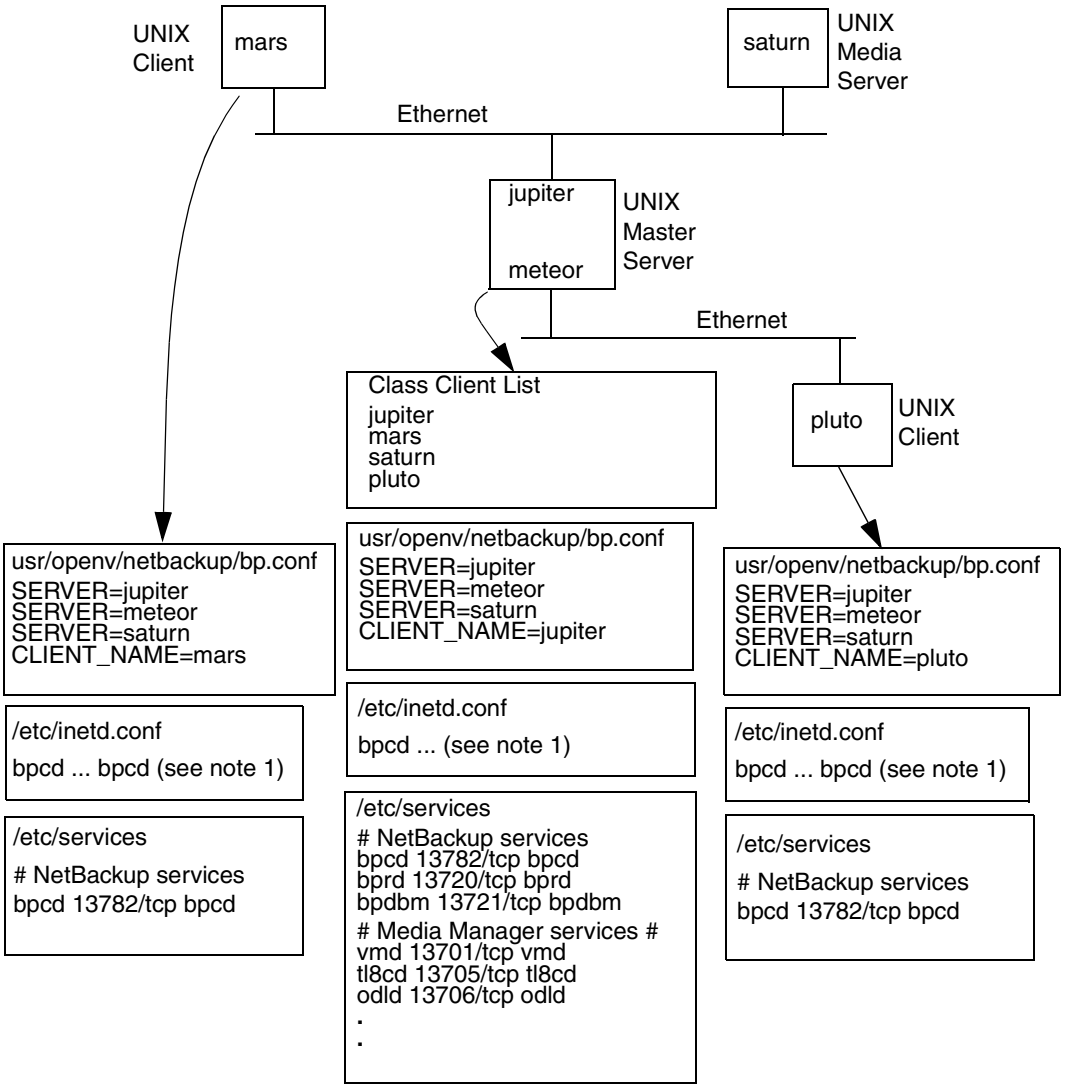
The NetBackup server list for the other systems also have entries for both the jupiter and meteor interfaces. This is recommended in order to keep the server entries the same on all clients and servers in the configuration. It would be adequate to list only the master-server name for the local network interface to the client system or media server (for example, meteor for pluto).

For the network shown, the differences mentioned for the class client list and the server list is the only unique configuration required. Assuming that all the standard networking files (for example, the hosts file, WINS, NIS, DNS, and routing tables) are set up correctly, all required network connections can be made.

If the master server system is a type of router that hides the name of the originating host when routing requests between networks, you see the same type of restore problem discussed in example 4. For example, if pluto were on FDDI (token ring), the master server would use meteor as the peername when it forwarded the request to NetBackup. NetBackup would then interpret the request as coming from a host named meteor, which was not in the client list, and the restore would fail.

The solution, in this case, is also identical to that discussed in "UNIX Example 4: Clients in Multiple Networks" on page 43.

Example 5: Server Connects to Multiple Networks



Notes: 1. The complete inetd.conf entry is:

bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd

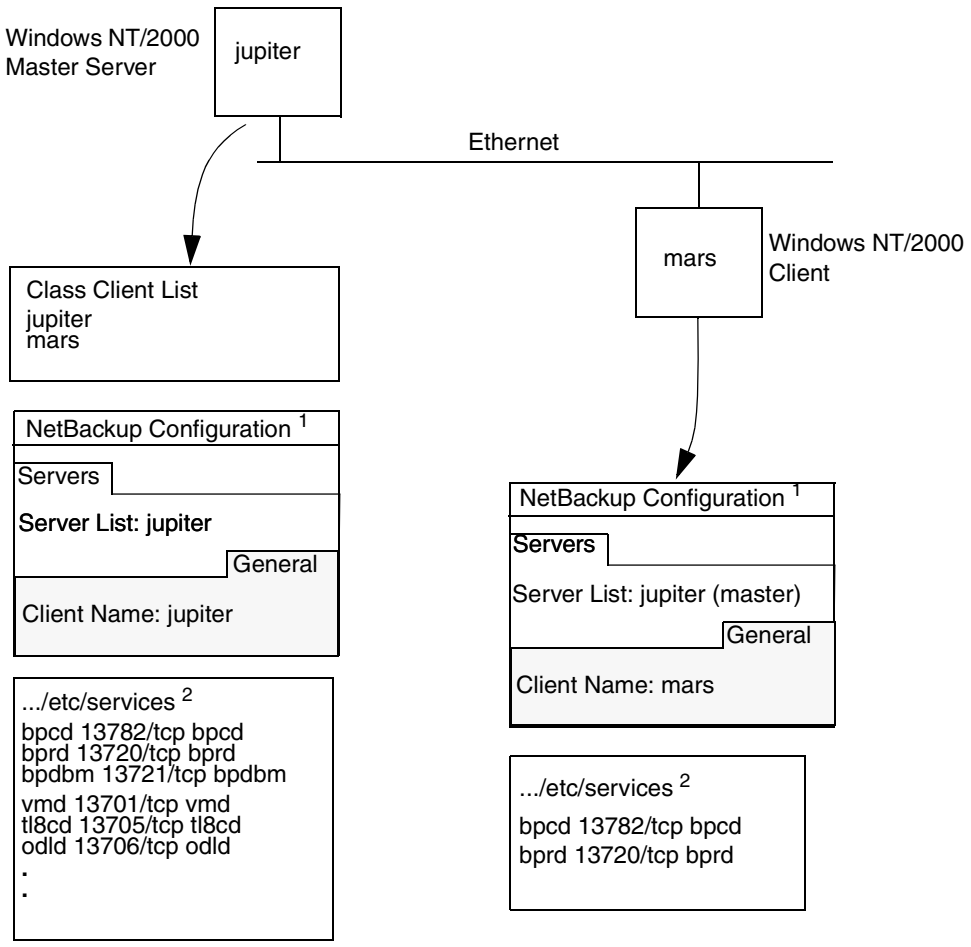
2. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the /etc/hosts file and NIS, and DNS (if used).

Host Name and Service Entry Examples- Windows NT/2000

Windows NT/2000 Example 1: Master Server and Client

The example network in the following figure shows a Windows NT/2000 master server with one Windows NT/2000 client.

Example 1: Windows NT/2000 Master Server and Client



Notes: 1. The NetBackup Client Properties dialog also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings that must be the same as the bpcd and bprd settings in the services file.

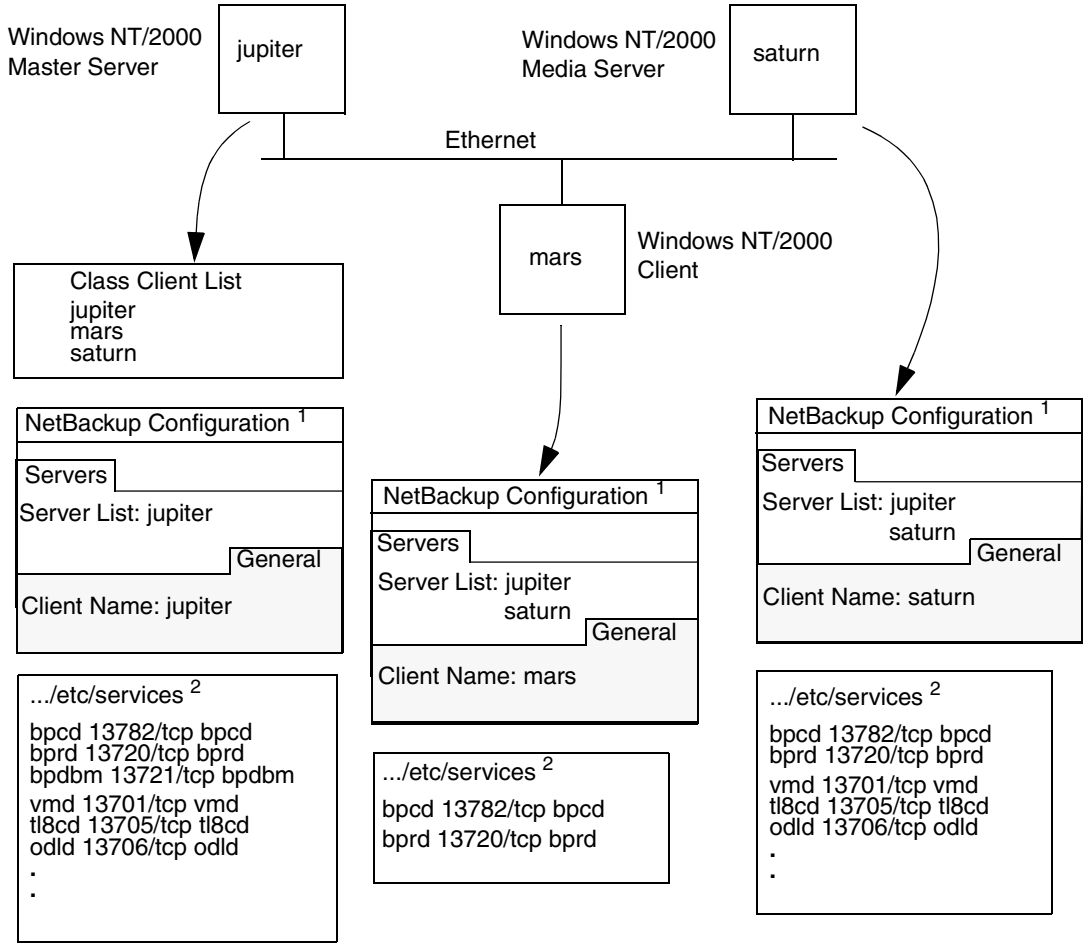
2. The complete path to the Windows NT/2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the %SystemRoot%\system32\drivers\etc\hosts file and also WIN and DNS (if used).

Windows NT/2000 Example 2: Master and Media Servers

The network in this example (see the next figure) is the same as the previous one except that it includes a NetBackup media server named saturn. The difference to note is the addition of a server list for saturn on all the systems. Jupiter is designated as the master.

Example 2: Windows NT/2000 Master and Media Servers



Notes: 1. The NetBackup Client Properties dialog also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings that must be the same as the bpcd and bprd settings in the services file.

2. The complete path to the Windows NT/2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the %SystemRoot%\system32\drivers\etc\hosts file and also WIN and DNS (if used).

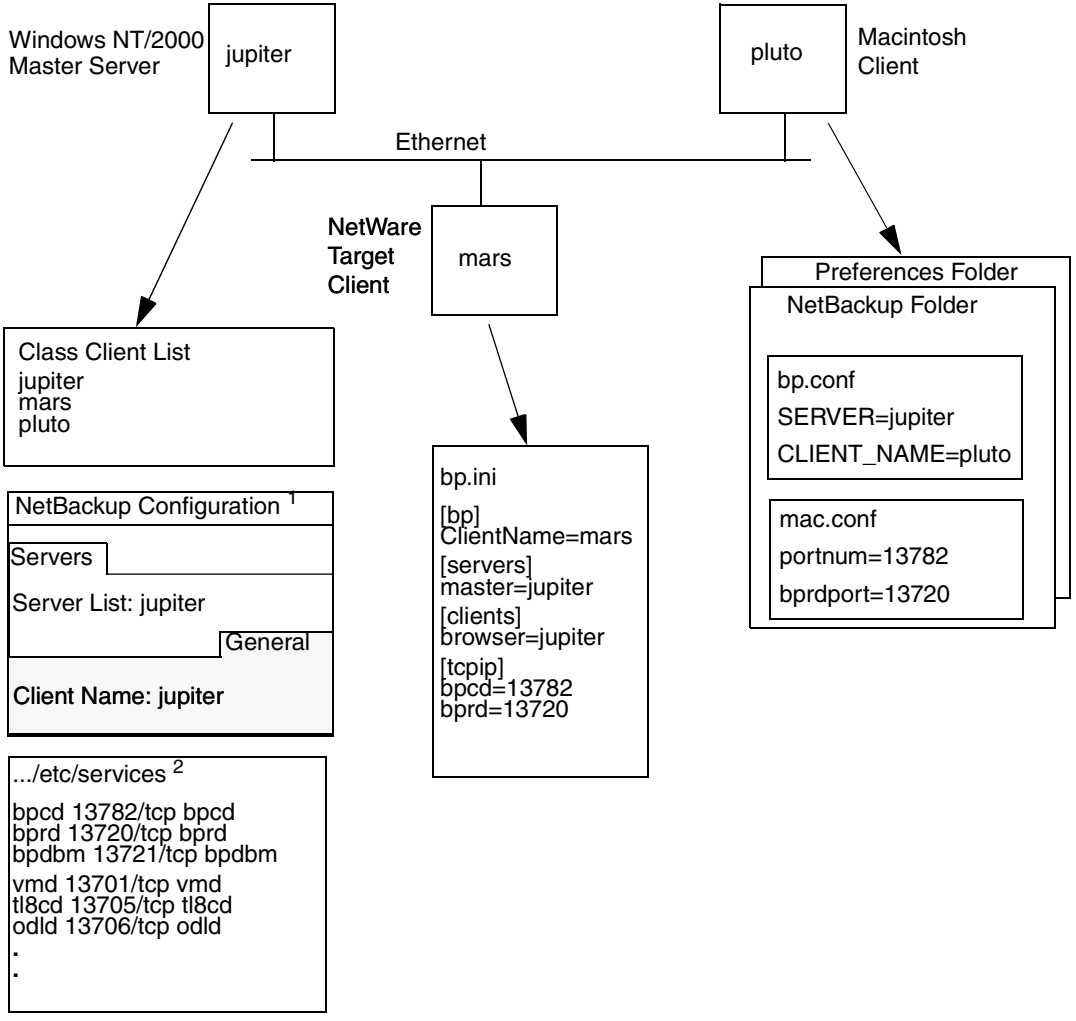
Windows NT/2000 Example 3: NetWare and Macintosh Clients

The network in the next figure shows a NetBackup master server with NetWare and Macintosh clients.

Note the following about this configuration:

- The server configuration is the same as with for other clients.
- Configuration entries on the Macintosh client are in the `mac.conf` and `bp.conf` files.
- Configuration entries on the NetWare client are in the `openv\netback\bp.ini` file.

Example 3: PC Clients



Notes: 1. The NetBackup Client Properties dialog also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings that must be the same as the bpcd and bprd settings in the services file.

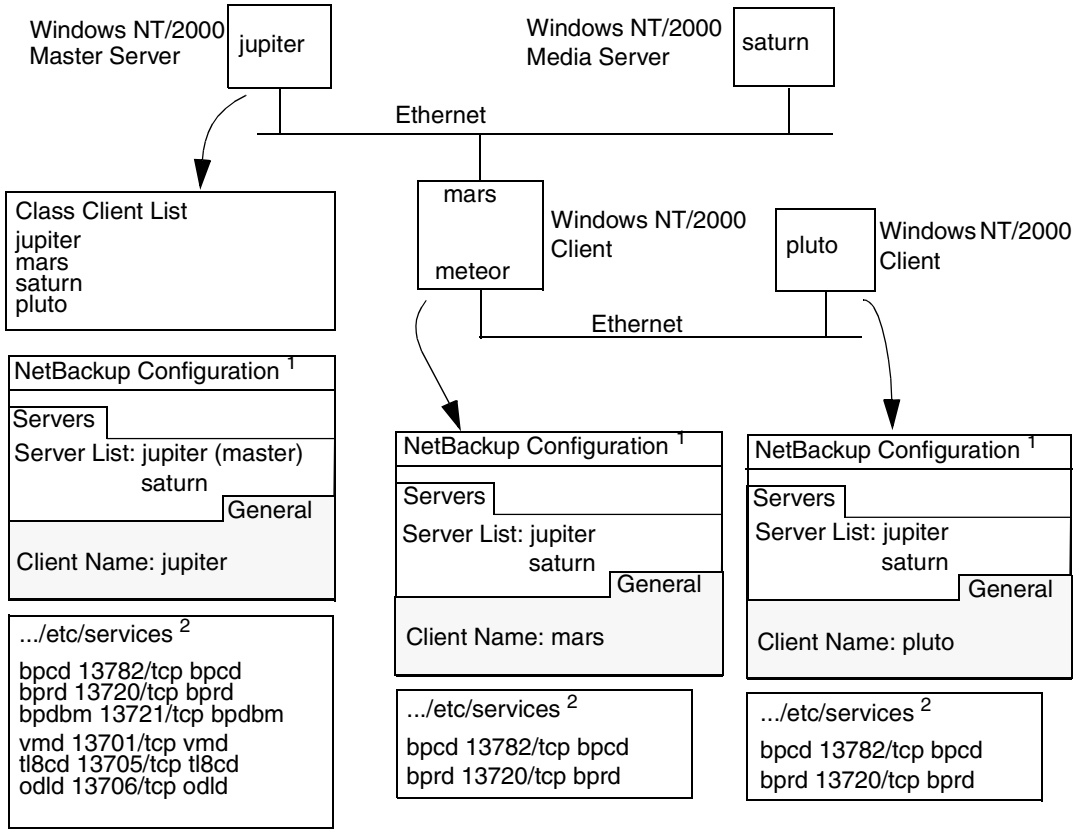
2. The complete path to the Windows NT/2000 \etc\services file is:
   %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the %SystemRoot%\system32\drivers\etc\hosts file and also WIN and DNS (if used).

Windows NT/2000 Example 4: Clients in Multiple Networks

The network in this example shows a client (mars/meteor) that is a router to clients in another network. The client's host name on the master server side is mars and the host name presented to the client pluto is meteor.

Example 4: Clients in Multiple Networks



Notes: 1. The NetBackup Client Properties dialog also has a Network tab with "NetBackup client service port (BPCD)" and "NetBackup request service port (BPRD)" settings that must be the same as the bpcd and bprd settings in the services file.

2. The complete path to the Windows NT/2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the %SystemRoot%\system32\drivers\etc\hosts file and also WIN and DNS (if used).

First, we examine the configuration of the router system. The NetBackup class client list shows this system as mars because that is the name of the interface to the master server. There is no special configuration to note other than the client name setting. This name must be set to mars, because this is the name that the master server recognizes.

The second client, pluto, is also configured no differently than if it were in the same network as the master server. Assuming that all the standard networking files (for example, hosts, DNS, WINS, and routing tables) are set up correctly, all the required network connections can be made.

There would be a problem, however, with restoring files from pluto if the mars/meteor system were a type of router that hides the name of the originating host when it routes requests between the two networks. A router between an Ethernet and a token ring network exhibits this behavior.

To illustrate what occurs, assume that pluto is on FDDI (token ring) and the server is on Ethernet. If a user on pluto starts a restore, the router could use the name of its network interface to pluto (meteor) as the peername when it forwards the request to the server. The server interprets the request as coming from a host named meteor and does not allow the restore because meteor is not in the client list.

To resolve this problem, the administrator creates an `altnames` directory on the master server and adds a file for meteor to that directory.

On a Windows NT/2000 NetBackup server, the file is:

install_path`\NetBackup\db\altnames\meteor`

Then, the administrator adds the following line to this file:

```
pluto
```

The master server now recognizes, as legitimate, restore requests that show a peername of meteor and client name of pluto. Refer to the *NetBackup System Administrator's Guide-Windows NT/2000* for more information on `altnames` configuration.

Regardless of the type of router, the configuration for the media server, saturn, is still the same as in example 2. If a media server is involved in a backup or restore for pluto, the master server provides the correct peername and client name for the media server to use in establishing connections.

Windows NT/2000 Example 5: Server Connects to Multiple Networks

The network in this example (see the next figure) shows a NetBackup server (jupter/meteor) that has two Ethernet connections and clients in both networks. The server's hostname is mars on one network and meteor on the other.

The first thing to note about this configuration is that the NetBackup class client list specifies jupiter as the client name for the master server. The list could show either jupiter or meteor but not both.

Another important item to note is the configuration of the NetBackup server list.

The NetBackup server list on the master server has entries for both jupiter and meteor. The reason for both names is that when the server does a backup, it uses the name associated with the client it is backing up. For example, it uses the meteor interface when backing up pluto and the jupiter interface when backing up mars. The current server entry (master server name) is jupiter because that is the name used to back up the client on the master server.

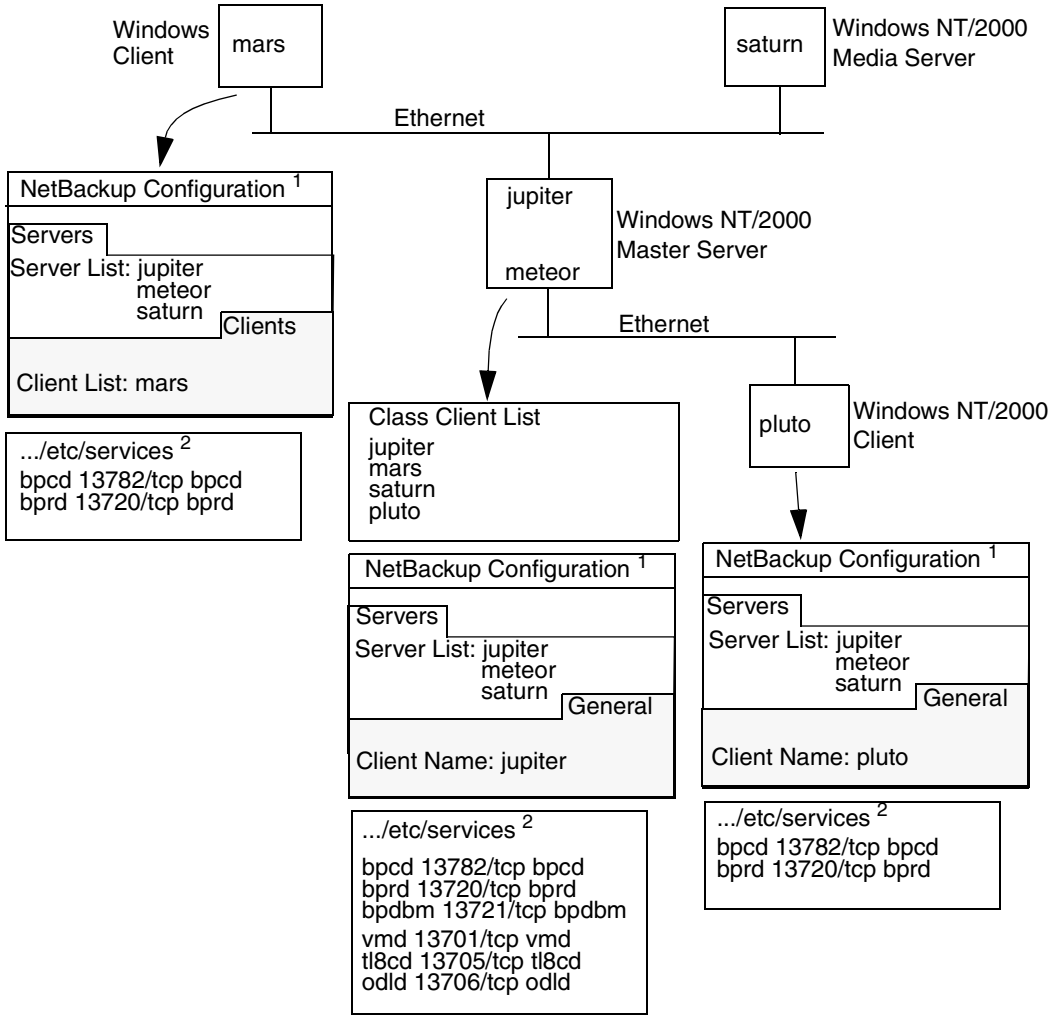
The NetBackup server list for the other systems also have entries for both the jupiter and meteor interfaces. This is recommended in order to keep the server entries the same on all clients and servers in the configuration. It would be adequate to list only the master-server name for the local network interface to the client system or media server (for example, meteor for pluto).

For the network shown, the differences mentioned for the class client list and the server list is the only unique configuration required. Assuming that all the standard networking files (for example, the hosts file, WINS, DNS, and routing tables) are set up correctly, all required network connections can be made.

If the master server system is a type of router that hides the name of the originating host when routing requests between networks, you see the same type of restore problem discussed in example 4. For example, if pluto were on FDDI (token ring), the master server would use meteor as the peername when it forwarded the request to NetBackup. NetBackup would then interpret the request as coming from a host named meteor, which was not in the client list, and the restore would fail.

The solution, in this case, is also identical to that discussed in "Windows NT/2000 Example 4: Clients in Multiple Networks" on page 53.

Example 5: Server Connects to Multiple Networks



Notes: 1. The NetBackup Client Properties dialog also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings that must be the same as the bpcd and bprd settings in the services file.

2. The complete path to the Windows NT/2000 \etc\services file is:
   %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this could include the %SystemRoot%\system32\drivers\etc\hosts file and also WIN and DNS (if used).

Using the Configure - NetBackup Window

Note Available only in the NetBackup Administration interface for Windows NT/2000.

The Configure - NetBackup window in the NetBackup Administration interface on Windows NT/2000 provides access to many configuration settings for NetBackup clients and servers. For example, you can modify the server list, e-mail notification settings, and various timeout values for servers and clients. The following are general instructions for using this window. For more information, see the online help or the *NetBackup System Administrator's Guide - Windows NT/2000*.

1. Start the NetBackup Administration interface on a Windows NT/2000 server or an administration client.
2. Click Configure NetBackup on the Start menu.
3. Select the servers or clients where you want to make the change.
4. Click the Properties command on the File menu.
5. In the properties dialog box that appears, select the appropriate tab and make your change.

Many procedures in this guide also refer to the NetBackup Configuration dialog box in the Backup, Archive, and Restore interface on Microsoft Windows clients. This dialog box lets you change NetBackup configuration settings only for the local system where you are running the interface program. Most settings in the NetBackup Configuration dialog box are also available in the Configure - NetBackup window.

Using the Logs and Reports 3

NetBackup produces the following categories of information that you can use for troubleshooting problems.

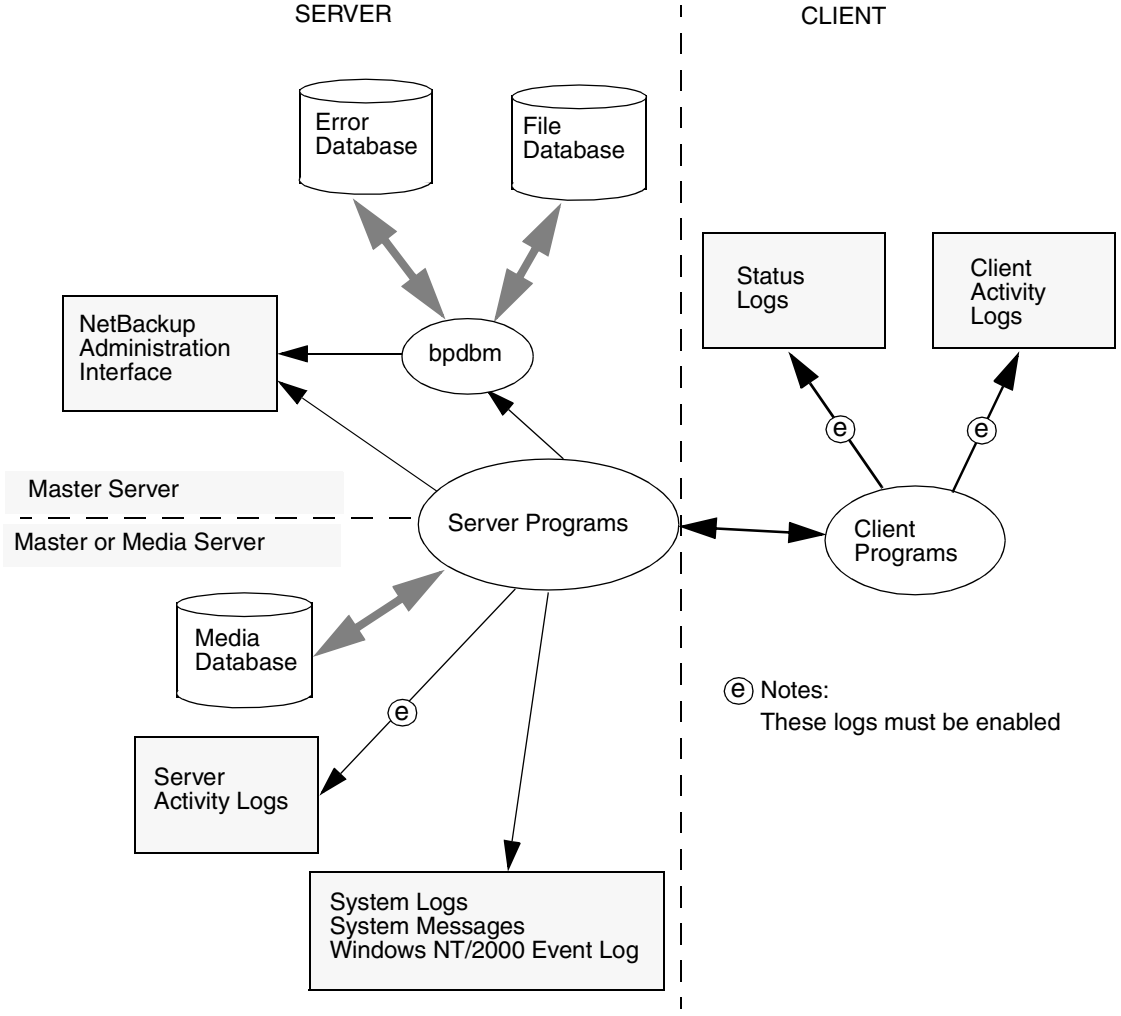
- Reports
- Status for User Operations
- System Logs
- Activity Logs
- Media Manager Logs
- Windows NT/2000 Event Viewer Logging Option
- Troubleshooting the Java Administration Interface

Note The format of the entries in the NetBackup logs is subject to change without notice.

The following figure shows whether this information is available on the client or server and the processes involved in making the information available. The remaining topics in this chapter describe the reports and logs shown on the figure.

See Appendix A for more information on the programs and daemons mentioned in this figure and elsewhere in this chapter.

Note The term *media server,* as distinct from *master server* or *server,* does not apply to the NetBackup BusinesServer product. When troubleshooting a BusinesServer installation, please ignore any references to media server in this guide.

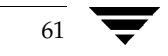


Reports

NetBackup provides a set of standard reports that gives you most of the status and error information you need. To run these reports, use the NetBackup administration interface (see the *NetBackup System Administrator's Guide* for instructions). The following table provides a brief description of the reports.

Table 2. NetBackup Reports

Report	Description
Backup Status	Status and error information on backups and archives completed within the specified time period. Environment variables allow modification of character lengths of some fields.
Media Reports	Provides the following reports about the media: ◆ Media Lists - Shows information about volumes that NetBackup has used for backups or archives. This report does not show information for disk storage units. ◆ Media Contents - Lists the backup IDs that are on a single volume. The information is read directly from the media. This report does not show information for disk storage units. ◆ Images on Media - Shows the contents of media as recorded in the NetBackup file database. This report shows information for any type of storage unit, including disk. ◆ Media Log Entries - Lists the media errors that have been recorded. This information is a subset of the All Log Entries report. ◆ Media Summary - Summarizes active and nonactive volumes and groups them according to expiration date. The report shows the expiration date and the number of volumes that are at each retention level. ◆ Media Written - Identifies volumes that have been used for backups or archives within the specified time period. This report does not show media used for image duplication if the original image was created prior to the specified time period.
Client Backups	Detailed information on backups and archives completed within the specified time period.
Problems	Problems that the server has logged during the specified time period. This information is a subset of the information in the All Log Entries report.
All Log Entries	All log entries for the specified time period.



Status for User Operations

NetBackup allows you to view status on the progress of user operations. See the NetBackup user guides for instructions

System Logs

On UNIX, the NetBackup server daemons and programs occasionally log information through `syslogd`, which then shows a message or writes the information in an appropriate system log or the console log. See the `syslogd` man page for the locations of system log messages on your system.

On Windows NT/2000, the NetBackup services and programs log information to the Event Viewer Application log. Look for messages pertaining to NetBackup in these logs.

Activity Logs

If a problem requires more information than is available through the normal logs and reports, you can enable activity logs that show detailed information about specific processes. To enable activity logging for a process, create a directory for its logs as explained in the following topics. Each process creates logs in its own logging directory. The logs that are available depend on whether the system is a server or a client.

Activity Logs on Servers

To enable activity logging on NetBackup servers, create the appropriate directories under:

`/usr/openv/netbackup/logs` (on UNIX)

install_path`\NetBackup\logs` (on Windows NT/2000)

The table below lists the activity log directories that apply to servers. When these directories exist, NetBackup creates log files in the directory for the associated process.

See Appendix A for more information on the programs and daemons that write the logs. (On UNIX systems, also refer to the `README` file in the `/usr/openv/netbackup/logs` directory).

On a Windows NT/2000 server, you can create all of the NetBackup activity log directories at once by running the following batch file:

install_path`\NetBackup\Logs\mklogdir.bat`

Note Media servers have only the `bpbrm`, `bpcd`, `bpdm`, and `bptm` activity logs.

Table 3. NetBackup Server Activity Logs

Activity Log Directory	Associated Process
admin	Administrative commands.
bpbrm	NetBackup backup and restore manager.
bpcd	NetBackup client daemon.
bpdbjobs	NetBackup jobs database manager program.
bpdm	NetBackup disk manager.
bpdbm	NetBackup database manager. This process runs only on master servers.
bpjava-msvc	NetBackup-Java application server authentication service started by inetd during startup of the NetBackup Java interface applications. This program authenticates the user that started the application.
bpjava-usvc	NetBackup program started by bpjava-msvc upon successful login through the Login dialog box that is presented when a NetBackup-Java interface is started. This program services all requests from the Java administration and user interfaces on the host where bpjava-msvc is running.
bprd	NetBackup request daemon.
bpsched	NetBackup backup scheduler. This process runs only on master servers.
bptm	NetBackup tape or optical media management process.
user_ops	The user_ops directory is created during the install of NetBackup on all servers and clients. The NetBackup Java interface programs use it for temporary files and for job and progress log files generated by the user backup, archive, and restore program (jbpSA). This directory must exist for successful operation of any of the Java programs and must have public read, write and execute permissions. user_ops will contain a directory for every user that is using the Java programs.
xbpadm	xbpadm (X Windows based administrator utility for NetBackup)
xbpmon	xbpmon (X Windows based NetBackup job monitor)

The following is a list of facts to be familiar with before using activity logs:

- NetBackup retains activity logs for the number of days you specify with the Duration to Keep Logs global attribute (28 days by default) and then deletes them. On UNIX, NetBackup deletes the logs on the master server, media servers and clients. For instructions on changing Duration to Keep Logs, see the *NetBackup System Administrator's Guide* - (UNIX or Windows NT/2000, whichever applies).

Note NetBackup can automatically delete the activity logs only if all clients are running at least NetBackup 3.0 software. If any clients are running an earlier version of NetBackup and you do not upgrade them, you must manually delete the activity logs.

- Activity logs can grow very large. Enable them only if unexplained problems exist and delete both the logs and the associated directory when they are no longer needed.
- Each activity log is kept in a separate subdirectory under:

  `/usr/openv/netbackup/logs` (on UNIX servers and clients)

  install_path`\NetBackup\Logs` (on Windows NT/2000 servers)

  Activity logging takes place only if you create the subdirectory where the process can store its logs.
- A process creates one activity log file per day.

  On UNIX, the file names created are of the form:

  log.*mmddyy*

  For example:

  ```
  log.140898
  ```

  On Windows NT/2000, the file names created are of the form:

  mmddyy.log

  For example:

  ```
  040198.log
  ```
- An activity log file is created when the process begins. Therefore, you must create the directory for an activity log before the process starts.
- To increase the amount of information that processes write in the logs:
  - On UNIX systems, define the string `VERBOSE` in the file:

    `/usr/openv/netbackup/bp.conf`

    `VERBOSE` by itself sets the verbose value to 1. To set a higher value, for more logging detail, enter `VERBOSE = 2` or a higher value.

Caution High verbose values can cause debug logs to become extremely large.

The UNIX commands that start some daemons and programs (for example, `bprd`) also have verbose options. To enable verbose logging for only specific processes, specify the verbose flag (if available) when starting the program or daemon.

- On Windows NT/2000 systems, set the Verbose level to 1 or more on the TroubleShooting tab of the NetBackup Configuration dialog box. To open this dialog box, start the client-user interface and click Configure on the Actions menu.

Activity Logs on UNIX Clients

To enable activity logging on UNIX clients, create the appropriate directories under:

`/usr/openv/netbackup/logs`

The following table lists the activity log directories that apply to UNIX clients. Also, see the list of facts to be familiar with under "Activity Logs on Servers" on page 62, because information also applies to UNIX clients.

Note Create the directories with access modes of 777 or user processes cannot write to the log files.

Table 4. UNIX Client Activity Logs

Activity Log Directory	Associated Process
`bp`	Menu driven client-user interface program.
`bparchive`	Archive program. These activity logs are also useful for debugging `xbp` and `bp` processes.
`bpbackup`	Backup program. These activity logs are also useful for debugging `xbp` and `bp` processes.
`bpbkar`	Program used to generate backup images.
`bpcd`	NetBackup client daemon.
`bpjava-msvc`	See Table 3.
`bpjava-usvc`	See Table 3.
`bplist`	Program that lists backed up and archived files. This activity log is also useful for debugging `xbp` and `bp` processes.
`bpmount`	Program that determines local mount points and wildcard expansion for Multiple Data Streams.
`bprestore`	Restore program. These activity logs are also useful for debugging `xbp` and `bp` processes.
`bphdb`	Program used to start `obackup` to back up Oracle databases. See the *NetBackup for Oracle System Administrator's Guide* for more information.

Table 4. UNIX Client Activity Logs (continued)

Activity Log Directory	Associated Process
db_log	For more information on these logs, see the NetBackup guide for the database-extension product that you are using.
tar	tar process during restores.
user_ops	See Table 3.

Activity Logs on PC Clients

Activity Logs on Windows and Netware Clients

To enable detailed activity logging on Microsoft Windows or NetWare target clients, create the appropriate directories in the following locations:

Note These are the default locations in which to place these directories. You can specify another location during client installation (see the user guide for the respective client).

- Windows NT/2000, 98, 95 clients - C:\VERITAS\NetBackup\Logs\
- NetWare clients - SYS:\OPENV\NETBACK\LOGS\

The following table lists the activity log directories that apply to the above clients:

Table 5. PC Client Activity Logs

Activity Log Directory	NetBackup Client	Associated Process
bp	NetWare target	Client-user interface program for NetWare.
bpinetd	Windows NT/2000	Client service logs. These logs have information on the bpinetd32 process.
bparchive	Windows NT/2000, 98, 95	Archive program that is run from the command line.
bpbackup	Windows NT/2000, 98, 95	Backup program that is run from the command line.
bpbkar	Windows NT/2000	Backup and archive manager. These logs have information on the bpbkar32 process.

Table 5. PC Client Activity Logs

Activity Log Directory	NetBackup Client	Associated Process
bpcd	All Windows and NetWare clients	NetBackup client daemon. These logs have information on communications between the server and client. On NetWare and Windows 98 and 95 clients, these logs also contain the log information for the backup and restore processes.
bplist	Windows NT/2000, 98, 95	List program that is run from the command line.
bpmount	Windows NT/2000, 98, 95	Program used to collect drive names on the client for multistreaming clients.
bprestore	Windows NT/2000, 98, 95	Restore program that is run from the command line.
bpsrv	NetWare nontarget	NetBackup service utility. This program allows the system with the user interface to communicate with the NetBackup for NetWare client.
nbwin	Windows 98, 95	Client-user interface program for Windows 98/95.
nbwin	Windows NT/2000	Client-user interface program for Windows NT/2000.
tar	Windows NT/2000	tar process. These logs have information about the tar32 process.
user_ops	Windows NT/2000, 98, 95	See Table 3.

Before using the activity logs, note the following:

- For Windows clients, logs are kept for the number of days specified in the Backup, Archive, and Restore utility, under the Actions menu, Configure, General tab: "Keep status of user-directed backups, archives, and restores for." For NetWare clients, logs are kept the number of days specified in file openv\netback\bp.ini (under Keep_Log_Days).

  The currently active logs have names of the form:

  mmddyy.log

  For example, 120198.log.

- You can increase the amount of information that processes write in the logs.

- On Windows clients, set the debug level on the TroubleShooting tab of the NetBackup Configuration dialog. For instructions, see the NetBackup user guide for the client.
- On NetWare clients, change the value of the `level` and `tcp` parameters in the debug section of the `bp.ini` file. For instructions, see the NetBackup user guide for the client.

Note Increasing the log level can cause the logs to grow very large, so take this action only if unexplained problems exist.

Activity Logs on Macintosh Clients

There are two types of activity logs on Macintosh clients:

- `bpcd` logs, which are located in the `Preferences:NetBackup:Logs:bpcd` folder. These logs have information on `NetBackupBPCD`, which controls communications between the server and the client.
- `inetd` logs, which are located in the `Preferences:NetBackup:Logs:bpcd` folder. These logs have information on `NetBackupListen`.

`NetBackupBPCD` and `NetBackupListen` each create one activity log file per day. The file names for these log files are of the form:

log.*mmddyy*

For example:

```
log.110899
```

To increase the amount of information that these processes write in the logs, change the value of the `loglevel` parameter in the `mac.conf` file in the NetBackup folder. Increasing the log level can cause these logs to grow very large, so take this action only if unexplained problems exist.

NetBackup retains Macintosh activity logs for the number of days you specify with the `logexpire` parameter in the `mac.conf` file in the NetBackup folder. The default is seven days.

For more on changing the `loglevel` or the `logexpire` value, see the *NetBackup User's Guide - Macintosh*.

Media Manager Logs

Media Manager logging is different on UNIX than on Windows NT/2000.

On UNIX

Media Manager on a UNIX system automatically records robotic and network errors in the system logs by using `syslogd`. System log entries are also made when robotically controlled drives change between UP and DOWN states.

Note You must enable system logging to troubleshoot `ltid` or robotic software. See the `syslogd(8)` man page for information on setting up system logs.

If a problem requires more information, enable debug logging to the system logs by including the verbose option (`-v`) on the command that you use to start a daemon. This command can be:

- The `ltid` command that started the device management processes. If the `-v` option is included on the `ltid` command, all daemons started as a result also have the `-v` option in effect. (if you are using `xvmadm` and `xdevadm`, note that their options for starting `ltid` do not enable debug logging.)

  or

- A command to start a specific daemon (for example, `acsd -v`). Alternatively, put a VERBOSE entry in the Media Manager configuration file, `/usr/openv/volmgr/vm.conf`, and restart `ltid` (create the `vm.conf` file if necessary).

See the `syslogd` man page for the locations of system log messages. Errors are logged with LOG_ERR, warnings with LOG_WARNING, and debug information with LOG_NOTICE. The facility type is daemon.

To enable debug logging for the Media Manager Volume daemon (`vmd`), create the following directories before starting `vmd` (or stop and restart `vmd` after creating them):

`/usr/openv/volmgr/debug/daemon`

(Debug information on the daemon)

`/usr/openv/volmgr/debug/reqlib`

(Debug information on the process requesting the daemon)

If you are using `xvmadm`, you can enable debug logging for it by creating the following directory:

`/usr/openv/volmgr/debug/xvmadm`

Media Manager creates one log per day in each of the debug directories with file names of the form:

log.*mmddyy*

For example:

```
log.110894
```

To disable `vmd` debug logging, either delete the directory or rename it. These directories continue to accumulate information until you either rename or delete them.

Note On HP-UX, the `sysdiag` tool may provide obtain additional information on hardware errors. On DEC OSF/1 the `uerf` command may provide additional information on hardware errors.

On Windows NT/2000

On Windows NT/2000, Media Manager records robotic and drive errors in the Event Viewer Application log. Log entries are also made when drives change between the UP and DOWN states.

If a problem requires more information, increase the level of logging to the Event Viewer Application log by adding a `VERBOSE` entry to the following file:

install_path`\Volmgr\vm.conf`

In addition, you can enable debug logging for the NetBackup Volume Manager service by creating the following directories:

install_path`\Volmgr\debug\daemon`

(Debug information on the service)

install_path`\Volmgr\debug\reqlib`

(Debug information on the process requesting the service)

NetBackup creates one log per day in each of the above debug directories with file names of the form:

mmddyy.log

For example:

```
110894.log
```

To disable debug logging for the NetBackup Volume Manager service, either delete or rename the directories.

Windows NT/2000 Event Viewer Logging Option

NetBackup Windows NT/2000 master servers can be configured so messages from NetBackup reports are written to the Windows NT/2000 Event Viewer Application Log. This allows you to see these messages in the Application Log and also to use third party tools to monitor the Application Log for these messages.

To Enable the Logging Tool

1. Create the following file on the NetBackup master server:

   install_path\NetBackup\db\config\eventlog

2. Add an entry (optional) to the `eventlog` file that specifies the severity and type of NetBackup messages that are written. The following is an example:

   ```
   56 255
   ```

   The next topic explains the format of the entry. If you do not add an entry, a default value is used, which is also explained in the next topic.

eventlog File Entries

The `eventlog` entry has two parameters:

- The first parameter controls which messages NetBackup writes to the Application Log, based on severity level.
- The second parameter controls which type of messages NetBackup writes to the Application Log.

Both parameters are specified as decimal numbers and equate to a bitmap that expresses the values below:

Severity:

1 = Unknown

2 = Debug

4 = Info

8 = Warning

16 = Error

32 = Critical

Type:

1 = Unknown

2 = General

4 = Backup

8 = Archive

16 = Retrieve

32 = Security

64 = Backup Status

128 = Media Device

- If the file is empty, the default severity is Error (16) and the default type is Backup Status (64).
- If the file has only one parameter, it is used for the severity level and the default value of Backup Status (64) is used for the type.

Example

Assume you want to include all types of messages that have severity levels of warning, error, and critical. In this instance, the entry is:

56 255

Where:

56 = severity= the sum of warning, error, and critical (8 + 16 + 32)

255 = type = the sum of all types (1 + 2 + 4 + 8 + 16 + 32 + 64 +128)

The following is an example of a message written in the Windows NT/2000 Event Viewer Application Log:

```
16 4 10797 cacao bush bpsched backup of client bush exited with status
71
```

The meaning of each field is as follows (left to right):

severity - 16 (Error)

type - 4 (Backup)

jobid - 10797

server - cacao

client - bush

process - bpsched

text - backup of client bush exited with status 71

Troubleshooting the Java Administration Interface

Most errors that occur in the NetBackup Java Administration interface appear in an attention dialog. Those that appear elsewhere are Java exception errors (which are not documented in this guide); they may appear in the status line (bottom) of the NetBackup Administration window, or in the log file that contains `stdout` or `stderr` messages written by Java APIs or by the NetBackup Administration interface.

The following are the four kinds of error messages seen in the NetBackup Java Administration interface.

- NetBackup status codes and messages as documented in Chapter 4.

  Operations performed in the Java Administration interface can result in errors recognized in other parts of NetBackup. These errors usually appear exactly as documented in Chapter 4.

Note The error message is not always accompanied by a status code. You can find the status code by looking up the message in the alphabetical listing at the end of Chapter 4. Then use the status code to find the full description of the message in the first half of Chapter 4.

- NetBackup Java Administration interface: application server status codes and messages as documented in Chapter 4.

  These messages have status codes in the 500 range. Messages with status codes 500, 501, 502, 503 and 504 begin with "Unable to login, status:". Messages with status codes 511 and 512 may or may not begin with “Unable to login, status:".

  The message is not always accompanied by a status code (see the above note).

- Java exceptions

  These are generated by either the Java APIs or by NetBackup Administration APIs. These messages begin with the name of the exception. For example:

  ```
  java.lang.ClassCastException
  ```

  or

  ```
  vrts.nbu.NBUCommandExecutionException
  ```

  Java exceptions usually appear in one of three places:

  - In the status line (bottom) of the NB Administration window
  - In the log file generated by the `jnbSA` or `jbpSA` commands
  - When set up, in the output file of the Windows Display Console `.bat` file (see “Enabling Detailed Activity Logging” below, for more detail)

- Operating system errors

  Messages that do not match those documented in this manual are probably operating system errors.

Enabling Detailed Activity Logging

The NetBackup Java Administration interface is a suite of client-server applications that allow administration of remote NetBackup servers. All administration is accomplished via the *application server* of the NetBackup Java Administration interface. This application server is made up of an authentication service and a user service.

The login request from the login dialog is sent to the authentication service for validation. The user name and password have to be valid in the Windows/UNIX authentication files/process.

After validation, the authentication service starts a user service under the user's account. Thereafter, all NetBackup administrative tasks are performed through that instance of the user service.

On both UNIX and Windows NT/2000, the authentication service is the `bpjava-msvc` application and the user service is the `bpjava-usvc` application.

Some of the recommendations in Chapter 4 refer to enabling detailed activity logging and examining log files. These are the instructions for this activity.

1. On the NetBackup client (*) or server specified in the login dialog, create the `bpjava-msvc` and `bpjava-usvc` activity log directories in the `/usr/openv/netbackup/logs` directory (UNIX) or in *install_path*`\NetBackup\logs` (Windows NT/2000). Refer to Activity Logs earlier in this chapter for more information.

Note The NetBackup Java application server runs only on NetBackup UNIX clients. On Windows NT/2000, the NetBackup Java application server runs only on NetBackup master servers.

2. On the UNIX machine where you execute the `jnbSA` or `jbpSA` commands, add the following line to the `Launch.properties` or `JBPSimple.properties` file, respectively, in the `/usr/openv/java` directory.

   ```
   debugLevel=2
   ```

   The log file name is displayed in the xterm window where you executed the `jnbSA` or `jbpSA` commands.

3. If you are using the NetBackup Windows Display Console, add the following line to the `host_name.properties` file in the NetBackup Java installed folder (for example, `C:\Veritas\java`):

   ```
   debugLevel=2
   ```

4. If you are using the Windows Display Console, you should also add the following to the end of the last command in the `associate.bat` file in the NetBackup Java installed folder:

   ```
   > jnbdebug
   ```

   This redirects output to a file.

Status Codes and Messages 4

This chapter lists all the status codes and messages provided by NetBackup. There are two parts to the chapter:

- The first section, Status Codes, lists the status codes in numerical order and includes an explanation of what occurred along with a recommended action.
- The second section, Messages, lists the same status codes but sorts them alphabetically according to the message associated with them. Only the messages and status codes are included the second section.

If you see a status code without its associated message text, you can determine the message, its explanation and recommended action by using the `bperror` command:

`/usr/openv/netbackup/bin/admincmd/bperror -statuscode` ***statuscode*** `[-recommendation]`

where ***statuscode*** is the number of the message.

Example:

```
/usr/openv/netbackup/bin/admincmd/bperror -statuscode 150

termination requested by administrator
The process is terminating (or has terminated) as a direct result of a
request from an authorized user or process.
```

Status Codes

Note The term *media server*, as distinct from *master server* or *server*, does not apply to the NetBackup BusinesServer product. When troubleshooting a BusinesServer installation, please ignore any references to media server.

Status Code: 0

Message: the requested operation was successfully completed

Explanation: There were no problems detected with the requested operation.

Recommended Action: None, unless this was a database backup performed through a database extension product (for example, NetBackup for Oracle or NetBackup for SQL Server). In those instances, code 0 means the backup script that started the backup ran without error. However, you must check other status as explained in the related NetBackup manual to see if the database was successfully backed up.

Status Code: 1

Message: the requested operation was partially successful

Explanation: A problem that may require corrective action was detected during the requested operation.

Recommended Action: Check the All Log Entries report and also the progress log (if there is one).

Some of the problems that can show up under Status Code 1 are:

- A file or directory path that is more than 1023 characters long.
- Could not open a file.
- On a UNIX system, NetBackup could not get the link name of a file.
- On a UNIX system, NetBackup could not process a sparse file.
- Read error encountered in a file.
- File is of an unknown type.
- On clients using Open Transaction Manager (OTM) for open file management, the OTM cache may be full. See the recommended actions under status code 11.
- On a UNIX system, the `lstat` system call fails on a file that is eligible to be backed up. This may be a permission problem.
- On UNIX, a file could not be locked that has mandatory locking enabled.

Status Code: 2

Message: none of the requested files were backed up

Explanation: A backup or archive could not back up any of the files in the file list.

Recommended Action: Verify that the files exist and you have read access to them.

- Check to see if there is a trailing space on one or more of the filenames in the client's file list. Remove any inadvertent trailing characters (such as spaces or tabs).
- On UNIX clients, check to see if the files or directories would be excluded because of an entry in `/usr/openv/netbackup/exclude_list`.

- On PC clients, check the exclude list per the instructions in the user's guide for the client.
- On Windows NT/2000 clients, verify that the account used to start the NetBackup Client service has read access to the files.

  If you are backing up a network drive or a UNC (universal naming convention) path, use the Services application in the Windows NT/2000 Control Panel to verify that the NetBackup Client service does not start under the SYSTEM account. The SYSTEM account cannot access network drives.

  To back up network drives or UNC paths, change the NetBackup Client service startup to log in as a user that has permission to access network drives.

Status Code: 3

Message: valid archive image produced, but no files deleted due to non-fatal problems

Explanation: The backup portion of the archive command reported problems so the files were not deleted.

Recommended Action: Examine the progress log of the archive on the client to determine if you need to retry the archive after correcting the problem. If the problem is not serious and the files were backed up, you can manually delete the files. To verify which files were backed up, use the NetBackup client-user interface in restore mode and browse the files in the archive.

A possible cause for files not being deleted is that you do not have the necessary permissions. NetBackup cannot delete files unless you are either the user that owns the files, a superuser on UNIX, or an administrator on Windows NT/2000.

Status Code: 4

Message: archive file removal failed

Explanation: The backup portion of the archive completed was successful but the delete failed.

Recommended Action: Verify that you have permission to delete the files and that the read-only flag is not set for the files. On UNIX clients, verify that you have write permission to the directories that contain the files. Since the backup was successful, you can delete the files that were backed up (or have the system administrator delete the files if you do not have the necessary permissions).

Status Code: 5

Message: the restore failed to recover the requested files

Explanation: There were errors that caused the restore to fail.

Recommended Action:

1. Ensure that the client's server list contains entries for the master server and for any media servers that could be used during a backup or restore.

2. Examine the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.

3. On Windows NT/2000 and UNIX, check ownership and permission on directories where files will be restored.

4. Correct problems that you find and retry the restore.

Status Code: 6

Message: the backup failed to back up the requested files

Explanation: Errors caused the user backup to fail.

Recommended Action:

1. Verify that you have read access to the files. Check the progress log on the client for messages on why the backup failed. Correct problems and retry the backup.

2. On Windows NT/2000 clients, verify that the account used to start the NetBackup Client service has read access to the files.

3. On Macintosh clients, this code can be due to multiple backups being attempted simultaneously on the same client. Some possible solutions are:

   - Adjust the backup schedules.
   - If the client is only in one class, set the class attribute, Limit jobs per class, to 1.
   - Set the NetBackup global attribute, Maximum jobs per client, to 1 (note that this limits all clients in all classes).

4. For a UNIX database extension client (for example, NetBackup for Oracle), this can mean a problem with the script that is controlling the backup.

   Check the progress report on the client for a message such as "`Script exited with status code =` *number*" (the number will vary). The progress log also usually names the script.

   Check the script for problems. Also, check the troubleshooting logs created by the database extension. See the NetBackup guide that came with the database extension for information on the scripts and troubleshooting logs.

Status Code: 7

Message: the archive failed to back up the requested files

Explanation: Errors caused the user archive to fail.

Recommended Action: Verify that you have read access to the files. Check the progress log on the client for messages on why the archive failed. Correct problems and retry the archive.

On Windows NT/2000 clients, verify that the account used to start the NetBackup services has read access to the files.

Status Code: 8

Message: unable to determine the status of rbak

Explanation: On DomainOS clients, `rbak` is used to do restores. If `rbak` does not exit with a status message, NetBackup cannot determine whether the restore worked or not.

Recommended Action: Check for a new core file to see if `rbak` aborted. Check the `ps` output to see if `rbak` is hung. If so, kill it and try again. Check the progress log for any unusual messages from `rbak`.

Status Code: 9

Message: an extension package is needed but was not installed

Explanation: A NetBackup extension product is required in order to perform the requested operation.

Recommended Action: Install the required extension product.

Status Code: 10

Message: allocation failed

Explanation: Allocation of system memory failed because there is insufficient system memory available. This could be caused by the system being overloaded with too many processes and not enough physical or virtual memory.

Recommended Action: Free up memory by terminating unneeded processes that consume memory. Add more swap space or physical memory.

Status Code: 11

Message: system call failed

Explanation: A system call failed. This status code is used for a generic system call failure that does not have its own status code.

Recommended Action:

1. Check the All Log Entries and Problems reports to determine which system call failed and other information about the error.

2. A frequent cause is that the server's file system is full. For example, you may see a message similar to the following in the Problems report or `bpdbm` activity log:

```
06/27/95 01:04:00 romb romb  db_FLISTsend failed: system call failed (11)
06/27/95 01:04:01 romb romb  media manager terminated by parent process
06/27/95 01:05:15 romb romb  backup of client romb exited with status 11
       (system call failed)
```

   On UNIX systems, run a `df` command on the `/usr/openv/netbackup/db` directory.

   If the `df` command does not reveal the problem, check the `bpdbm` activity logs or do a `grep` for the message

   ```
   system call failed
   ```

   in `/usr/openv/netbackup/db/error/*`

   On Windows NT/2000 systems, verify that there is enough room in the disk partition where NetBackup is installed.

3. Verify that the system is not running out of virtual memory. If virtual memory is the problem, shut down unused applications or increase the amount of virtual memory.

   To increase virtual memory on Windows NT/2000, 98, and 95:

   a. Display the Control Panel.

   b. Double-click System.

   c. On the Performance tab, set Virtual Memory to a higher value.

4. Check for a semaphore problem. This error can be caused by the system not having enough semaphores allocated. This is most commonly seen on Solaris 2 servers when an RDBMS is also running.

   The symptoms of the problem vary. In some cases, error messages in the NetBackup log indicate a backup failure due to an error in semaphore operation; another symptom is the inability of the NetBackup Device Manager service Media Manager device daemon, `ltid`, to acquire a needed semaphore (this is the NetBackup Device Manager service on Windows NT/2000).

System requirements vary; thus, no absolute recommendations can be made. One customer running both NetBackup and ORACLE on their Solaris server made the following changes to their `/etc/system` file and then rebooted the system (`boot -r`); the changes were found to be adequate:

```
set semsys:seminfo_semmni=300
set semsys:seminfo_semmns=300
set semsys:seminfo_semmsl=300
set semsys:seminfo_semmnu=600
```

Set these attributes to a value great enough to provide resources to all applications on your system.

5. Check for a shared memory problem. This error can occur if the system cannot allocate enough shared memory. This usually occurs when you use multiplexing, which increases the shared memory requirements. A symptom is an entry similar to the following in a NetBackup log (or report).

   ```
   could not allocate enough shared memory
   ```

   If you see this type of message, refer to the vendor documentation for your platform for instructions on increasing the amount of shared memory on your system.

   Because system requirements vary, no absolute recommendations can be made, other than to use values great enough to provide resources to all applications. In at least one instance, however, the following was found to be adequate on a Sun platform:

   ```
   set shmsys:shminfo_shmmax=8388608
   set shmsys:shminfo_shmmin=1
   set shmsys:shminfo_shmmni=100
   set shmsys:shminfo_shmseg=10
   set semsys:seminfo_semmnu=600
   set semsys:seminfo_semmns=300
   ```

   After making the changes to the `/etc/system file` on the Sun platform and rebooting with `boot -r`, the problem was resolved. Note that in the above, `shminfo_shmmin` must be less than or equal to 100 for NetBackup processes to run.

6. Examine other activity logs or the progress log on the client.

7. If a backup on a Windows NT/2000 NetBackup client fails with status code 11 and the client is using Open Transaction Manager (OTM) for open file management, it is possible that the error was caused by the OTM cache file being full. If this is the case and `bpbkar` activity logs are turned on, a message similar to the following should appear at the end of the backup:

```
04/28/99 11:27:56 AM: [216]: ERR - OTM Error:0xe0001005
04/28/99 11:27:59 AM: [216]: INF - OTM Terminate - disabled for all
processes
```

```
04/28/99 11:27:59 AM: [216]: FTL - Backup operation aborted!
```

If this error is encountered, try one of the following (the first is preferred):

- Set maximum OTM cache size to zero (0); at run time, OTM will determine how much cache is needed and set it accordingly.
- Increase either the initial OTM cache size or the maximum OTM cache size on your own, depending on the requirements of your installation and your usage of OTM.

If resizing OTM cache does not fix the problem, you may not have enough free disk space.

Status Code: 12

Message: file open failed

Explanation: An open of a file failed.

Recommended Action: Check the NetBackup Problems report. Try to determine the file and why the error occurred. A possible cause is a permission problem with the file. For detailed troubleshooting information, create an activity log directory for the process that returned this status code. Then, retry the operation, and check the resulting activity log.

Status Code: 13

Message: file read failed

Explanation: A read of a file or socket failed. Possible causes include:

- I/O error reading from the file system.
- Read of an incomplete or corrupt file.
- Socket read failing. A socket read failure can be caused by a network problem or a problem with the process that is writing to the socket.

Recommended Action:

1. Check the NetBackup Problems report for clues on where and why the problem occurred.
2. For a FlashBackup client, check the `/var/adm/messages` log for errors like the following:

```
Mar 24 01:35:58 bison unix: WARNING: sn_alloccache: cache
/dev/rdsk/c0t2d0s3 full - all snaps using this cache are now unusable
```

This indicates that the cache partition is not large enough. If possible, increase the size of the cache partition. Or, if multiple backups are using the same cache, either reduce the number of concurrent backups by rescheduling some of them or reschedule the entire backup to a time when the file system is less active.

3. For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 14

Message: file write failed

Explanation: A write to a file or socket failed. Possible causes include:

- I/O error writing to the file system.
- Write to a socket failed. This can be caused by a network problem or a problem with the process reading from the socket.
- Writing to a full disk partition.
- The `bpfsmap` temporary directory (usually `/tmp`) became full (on Auspex FastBackup jobs).

Recommended Action:

- Check the NetBackup Problems report for clues on where and why the problem occurred.
- On Auspex FastBackup jobs (for NetBackup 3.0), increase the size of the `/tmp` partition; there is a TMPDIR file which can be created for NetBackup 3.1.1.
- For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.
- Make sure that routers, bridges, and other network devices are all at "full" duplex.
- Use a "sniffer" program to determine the number of packets being rejected and/or re-requested.
- On Windows NT/2000 systems, the client `bpbkar` log may contain a 10054 "Connection Reset Error"error (usually indicates a hardware error). Somewhere between the NetBackup client and server, the connection was reset. When NetBackup receives this error, it is unable to continue the backup. This error has been attributed to the following:
  - A hiccup in the network.
  - A bad network interface card on a NetBackup client.

- A bad network interface card on the NetBackup server.
- Faulty routers.
- Other applications interfering with NetBackup connections.

- On Novell systems, status code 14 has also been attributed to network issues. Try a "sniffer" program, as suggested above.

Status Code: 15

Message: file close failed

Explanation: A close of a file or socket failed.

Recommended Action: Check the NetBackup Problems report for clues on where and why the problem occurred. For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 16

Message: unimplemented feature

Explanation: The specified operation is unimplemented. This error should not occur through normal use of NetBackup.

Recommended Action: Save all error information and call customer support.

Status Code: 18

Message: pipe close failed

Explanation: Close of a pipe failed, when one process tries to start a child process.

Recommended Action: Check the NetBackup Problems report for clues on why the failure occurred. For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 19

Message: getservbyname failed

Explanation: A call to `getservbyname()` failed. The `getservbyname()` function uses the name of the service to find a service entry in the `services` file (or NIS services map on UNIX if it is configured).

Recommended Action:

1. Check the NetBackup Problems report for clues on why the failure occurred.

2. On a UNIX system, check that `/etc/services` and NIS services map (if applicable) have entries for the NetBackup services: `bpcd`, `bpdbm`, and `bprd`.

3. On a Windows NT/2000 system, verify that the `%SystemRoot%\system32\drivers\etc\services` file shows the correct entries for the NetBackup internet processes: `bpcd`, `bpdbm`, and `bprd`.

   Ensure that the NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog box match the settings in the `services` file. To display this dialog, start the Backup, Archive, and Restore interface and click Configure on the Actions menu. The values on the Network tab are written to the `services` file when the NetBackup Client service starts.

   Also, see "Verifying Host Names and Services Entries" on page 32.

4. Check the level of network activity. An overloaded network can cause this error.

5. If the above actions do not reveal the problem, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 20

Message: invalid command parameter

Explanation: One or more command parameters were not valid. This error can occur when a master and its media servers or a master server and a client have different levels of NetBackup installed. For example, if a NetBackup master server has NetBackup 3.2 and the media server has NetBackup 3.0.

This error can also occur if the wrong parameters are used when executing a command line.

Recommended Action:

1. Check the NetBackup Problems report for clues.

2. If the error occurs when executing a command on the command line, verify that the parameters are valid.

3. Compare the NetBackup version level on the server to that on the clients:

   - On UNIX NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.

- On Windows NT/2000 NetBackup servers, check the *install_path*\netbackup\version.txt file or the About NetBackup item on the Help menu.
- On Microsoft Windows clients, check the About NetBackup item on the Help menu.
- On NetWare target clients, check the Version entry in the bp.ini file.

  If the client software is earlier than 3.0, verify that the client is in a Standard type class.
- On Macintosh clients, check the version file in the bin folder in the NetBackup folder in the Preferences folder.

4. If the above actions do not reveal the problem, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 21

Message: socket open failed

Explanation: A socket open failed.

Recommended Action:

1. Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create activity log directories for the processes that returned this status code. Then, retry the operation and check the resulting activity logs.

2. On Sun Solaris, verify that all operating system patches are installed (see the Operating Notes section of the *NetBackup Release Notes*).

3. On Windows NT/2000, verify that the recommended service packs are installed.

Status Code: 22

Message: socket close failed

Explanation: A socket could not be closed.

Recommended Action:

1. Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create activity log directories for the processes that could have returned this status code. Then, retry the operation and check the resulting activity logs.

2. On Sun Solaris, verify that all operating system patches are installed (see the Operating Notes section of the *NetBackup Release Notes*).

3. On Windows NT/2000, verify that the recommended service packs are installed.

Status Code: 23

Message: socket read failed

Explanation: A read operation from a socket failed.

Recommended Action:

1. Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create activity log directories for the processes that could have returned this status code. Then, retry the operation and check the resulting activity logs.

2. Corrupt binaries are one possible cause for this error. For example, in one instance, the following was seen in the `bpsched` activity log.

```
get_num_avail_drives: readline failed: socket read failed (23)
get_stunits: get_num_avail_drives failed with stat 23
```

   Loading a fresh `bptm` from the install media resolved the problem.

3. On Sun Solaris, verify that all operating system patches are installed (see the Operating Notes section of the *NetBackup Release Notes*).

4. On Windows NT/2000, verify that the recommended service packs are installed.

5. This error may occur during a restore to a Novell client. Note the following possible actions:

   - By default, the value for Novell "Maximum Concurrent Disk Cache Writes" may be too low (for example, 50); Novell recommends setting it to 100. A value of 100 increases the speed and efficiency of disk cache writes by increasing the number of write requests that can be executed at one time.
   - Change to or add the following settings in the Novell `sys:system\autoexec.ncf` file:

```
SET Maximum Packet Receive Buffers = 4000
```

```
SET Maximum Directory Cache Buffers = 4000
SET Maximum Concurrent Disk Cache Writes = 2000
SET Maximum Concurrent Directory Cache Writes = 2000
SET Maximum Physical Receive Packet Size = 1514
```

Status Code: 24

Message: socket write failed

Explanation: A write operation to a socket failed.

Recommended Action:

1. Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create activity log directories for the processes that could have returned this status code. Then retry the operation and check the resulting activity logs.

2. A possible cause could be a high network load. For example, this has been seen in conjunction with `Cannot write to STDOUT` when a Windows NT/2000 system that is monitoring network load has detected a high load and sent an ICMP packet to other systems that says the route being used by those systems was disconnected. The log messages were similar to the following:

```
01/31/96 14:05:23 ruble crabtree.null.com from client
crabtree.null.com: ERR - Cannot write to STDOUT. Err no= 242: No route
to host
01/31/96 14:05:48 ruble crabtree.null.com successfully wrote backup id
crabtree.null.com_0823125016, copy 1, fragment 1, 440864 Kbytes at
628.538 Kbytes/sec
01/31/96 14:05:51 netbackup crabtree.null.com CLIENT crabtree.null.com
CLASS Remote3SysFullW  SCHED Sirius  EXIT STATUS 24 (socket write
failed)
```

3. On Sun Solaris, verify that all operating system patches are installed (see the Operating Notes section of the *NetBackup Release Notes*).

4. On Windows NT/2000, verify that the recommended service packs are installed.

5. This error may occur during a restore to a Novell client. Note the following possible actions:

   - By default, the value for Novell "Maximum Packet Receive Buffers" may be too low (such as 100). The restore performance may be improved by changing this value to 2000. To change it, issue "SET Maximum Packet Receive Buffers=<value>" at the console, or enter the value in either of the following Novell files: `sys:system\startup.ncf` or `sys:system\autoexec.ncf`.

- Change to or add the following settings in the Novell `sys:system\autoexec.ncf` file:

```
SET Maximum Packet Receive Buffers = 4000
SET Maximum Directory Cache Buffers = 4000
SET Maximum Concurrent Disk Cache Writes = 2000
SET Maximum Concurrent Directory Cache Writes = 2000
SET Maximum Physical Receive Packet Size = 1514
```

Status Code: 25

Message: cannot connect on socket

Explanation: A process timed out while connecting to another process for a particular operation. This problem can occur when a process tries to connect to the NetBackup request daemon (`bprd`) or database manager daemon (`bpdbm`) and the daemon is not running. (On Windows NT/2000, these daemons are the NetBackup Request Manager and NetBackup Database Manager services.) It can also occur if the network or server is heavily loaded and has slow response time.

Recommended Action:

1. On a UNIX NetBackup master server, verify that the `bprd` and `bpdbm` processes are running. If these processes are not running, start them. On aWindows NT/2000 master server, verify that the NetBackup Request Manager and NetBackup Database Manager services are running. If these services are not running, start them.

   If the above processes are running, examine the All Log Entries report for the time of the failure to determine where the failure occurred.

   - If you cannot view the report, or you get a "`cannot connect on socket`" error when trying to view it, verify again that the NetBackup Database Manager daemon (or service) is running. Then, create an activity log directory for `bpdbm`, retry the operation, and check the resulting activity log.
   - If you can view the report and have not found an entry related to this problem, create activity log directories for the related processes that were running when the error first appeared (this process will frequently be `bpbrm`). Then, retry the operation and check the resulting activity logs.

2. Verify that the server list specifies the correct master server.

   - On Windows NT/2000, 98, and 95 systems, the master server is designated as CURRENT on the Servers tab in the Specify NetBackup Machines dialog. To display this dialog box, start the Backup, Archive, and Restore interface and click Specify NetBackup Machines on the Actions menu.
   - On UNIX, and Macintosh systems, the master server is the first `SERVER` entry in the `bp.conf` file.

- On NetWare target and OS/2 clients, the master server name is the first `SERVER` entry in the `bp.ini` file.
- Make sure all recommended NetBackup patches have been installed. Check the VERITAS support web site for current patch information. (Go to www.support.veritas.com, then select "NetBackup" followed by "files and updates".)
- If failure occurs when executing a user-directed backup from a client, make sure a user-directed backup schedule exists at the master server.
- When working with NetBackup database extensions, make sure that the applicable database product has the correct permissions allowing NetBackup to write to the progress log on the client.
- On UNIX systems, if bpdbm is dying when the shutdown script is executed on a slave server, carefully read the `K77netbackup` script (in `/usr/openv/netbackup/bin/goodies`) for details on how to prevent this problem.

If you change the server list on a master server, stop and restart the NetBackup database manager and request daemons (UNIX) or the NetBackup Database Manager and NetBackup Request Manager services (Windows NT/2000).

3. Check the `services` file.

On UNIX, verify that the `/etc/services` file (and NIS services if NIS is used) has entries for the NetBackup services: `bpcd`, `bpdbm`, and `bprd`.

On Windows NT/2000, verify that the `%SystemRoot%\system32\drivers\etc\services` file has the correct entries for `bpcd`, `bpdbm`, and `bprd`.

Also, verify that the NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog match the settings in the `services` file. To display this dialog, start the Backup, Archive, and Restore interface and click Configure on the Actions menu. The values on the Network tab are written to the `services` file when the NetBackup Client service starts.

Also, see "Verifying Host Names and Services Entries" on page 32.

4. On Sun Solaris, verify that all operating system patches are installed (see the Operating Notes section of the *NetBackup Release Notes*).

5. On Windows NT/2000, verify that the recommended service packs are installed.

Status Code: 26

Message: client/server handshaking failed

Explanation: A process on the server encountered an error when communicating with the client. This error indicates that the client and server were able to initiate communications, but encountered difficulties in completing them. This problem can occur during a backup or a restore.

Recommended Action: Determine which activity encountered the handshake failure by examining the All Log Entries report for the appropriate time period. Determine the client and server that had the handshake failure.

For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 27

Message: child process killed by signal

Explanation: A child of the process reporting this error was killed. This can occur because the backup job was terminated or the child process was terminated by another error. This problem can also occur if a NetBackup process was terminated through Task Manager or another utility.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create an activity log directory for the process that you suspect of returning this status code. Then, retry the operation and check the resulting activity log.

Status Code: 28

Message: failed trying to fork a process

Explanation: A fork of a child process failed (on UNIX) or a CreateProcess failed (on Windows NT/2000). This may be due to:

- An overloaded system
- Insufficient swap space or physical memory
- Too many processes running on the system

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create activity log directories for the processes that you suspect of returning this status code. Then, retry the operation and check the resulting activity logs.

Status Code: 29

Message: failed trying to exec a command

Explanation: A command could not be executed. This can occur because the permissions of the command do not allow it to be executed, or there is lack of system resources such as memory and swap space.

Recommended Action:

1. Check the NetBackup All Log Entries report for clues on where and why the failure occurred.
2. Check the permissions on the command to be executed.
3. For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 30

Message: could not get passwd information

Explanation: Could not get the `passwd` entry for a user.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create an activity log for the process that you suspect of returning this status code. Then, retry the operation and check the resulting activity log.

Status Code: 31

Message: could not set user id for process

Explanation: Could not set the user ID of a process to that of the requesting user. NetBackup executes client processes as the requesting user.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create an activity log directory for the process that you suspect of returning this status code. Then, retry the operation and check the resulting activity log.

Status Code: 32

Message: could not set group id for process

Explanation: Could not set the group ID of a process to the requesting user group. NetBackup executes client processes with the group ID of the requesting user.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create an activity log directory for the process that you suspect of returning this status code. Then, retry the operation and check the resulting activity log.

Status Code: 33

Message: failed while trying to send mail

Explanation: An E-mail notification of backup, archive, or restore results has failed. The E-mail could not be sent to the administrator's address as specified by the E-mail global attribute, or in the case of a UNIX client, an E-mail address specified with USEMAIL in the client's `bp.conf` file.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create an activity log directory for the process that you suspect of returning this status code. Then, retry the operation and check the resulting activity log.

Status Code: 34

Message: failed waiting for child process

Explanation: The `bpsched` process encountered a failure while waiting for a child process to complete.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create an activity log for the process that you suspect of returning this status code. Then, retry the operation and check the resulting activity log.

Status Code: 35

Message: cannot make required directory

Explanation: Could not create a required directory. Possible causes are:

- A process does not have permission to create the directory
- The path to the directory is not valid
- An IO error occurs
- There was no space available on the device containing the directory

Recommended Action:

1. Check the NetBackup All Log Entries report to determine which directory could not be created and why it could not be created. In particular, check for a full disk partition.

2. Check the permissions on the parent directory and verify that NetBackup services are started with a "Logon as" account that has permission to create the directory.

3. For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 36

Message: failed trying to allocate memory

Explanation: Allocation of system memory failed. This error occurs when there is insufficient system memory available. This could be caused by the system being overloaded with too many processes and there is not enough physical and virtual memory.

Recommended Action: Free up memory by terminating unneeded processes that consume a lot of memory. Add more swap space or physical memory.

Status Code: 37

Message: operation requested by an invalid server

Explanation: A request was made to the NetBackup request daemon (`bprd`) or NetBackup database manager daemon (`bpdbm`) by an invalid media server or Windows NT/2000 administration client. On Windows NT/2000, these daemons are the NetBackup Request Manager and NetBackup Database Manager services.

Recommended Action: Examine the NetBackup All Log Entries report for the time of this error to determine which system was trying to connect to the master server.

If the server is a valid media server, verify that the storage unit for the media server is defined. Also, verify that the server or Windows NT/2000 administration client has a server list entry on the master server.

If necessary, update the server list. On a UNIX master server, add a `SERVER =` *media_server_name* to the `bp.conf` file. *media_server_name* is the host name of the media server. On a Windows NT/2000 master server, add the media server to the list on the Servers tab in the Master Server Properties dialog (see "Using the Configure - NetBackup Window" on page 57).

If a server or Windows NT/2000 administration client has more than one host name (for example, if it has multiple network interfaces), verify that the master server has a server list entry for each of them.

If you change the server list on a UNIX master server, you must stop and then restart the NetBackup Request daemon (`bprd`) and NetBackup database manager daemon (`bpdbm`) for the changes to take effect. If you change the server list on a Windows NT/2000 master server, stop and then restart the NetBackup Request Manager and NetBackup Database Manager services.

Status Code: 38

Message: could not get group information

Explanation: Could not get the group entry describing a UNIX user group.

Recommended Action: Check the NetBackup Problems report for clues on why the error occurred. For detailed troubleshooting information, create an activity log directory for the process that returned this status code, retry the operation, and check the resulting activity log.

Status Code: 39

Message: client name mismatch

Explanation: The name that the client used in a request to the NetBackup server did not match the client name configured in the class on the server.

Recommended Action: Change either the NetBackup client name setting on the client (see the applicable NetBackup users guide) or the one in the class configuration on the server so the two match.

Status Code: 40

Message: network connection broken

Explanation: The connection between the client and the server was broken. This status code can also appear if the connection is broken between the master and media server during a backup.

Recommended Action:

1. Try pinging the client from the server. If this is not possible, check for loose connections or other network problems.

2. Verify that the server list settings are correct on both the client and the server. If the backup involves a media server, verify that these entries are correct on both the master and media server. For example, if a media server does not have a server list entry for the master, it does not accept connections from the master.

- On Windows NT/2000, 98, and 95 systems, the master server is designated on the Servers tab in the Master Server Properties dialog. To display this dialog, see "Using the Configure - NetBackup Window" on page 57.
- On UNIX, and Macintosh systems, the master server is the first `SERVER` entry in the `bp.conf` file.
- On NetWare target and OS/2 clients the master server name is the first `SERVER` entry in the `bp.ini` file.

If you change the server list on a UNIX master server, you must stop and then restart the NetBackup Request daemon (`bprd`) and NetBackup database manager daemon (`bpdbm`) for the changes to take effect. On Windows NT/2000, stop and restart the NetBackup Request Manager and NetBackup Database Manager services.

3. Status code 40 can also be due to the operator denying a mount request.

Status Code: 41

Message: network connection timed out

Explanation: The server did not receive any information from the client for too long a period of time.

Recommended Action:

1. On a UNIX or Windows NT/2000 clients, check for the following problems with the `bpbkar` client process.

- The `bpbkar` client process is hung on a file that has mandatory locking set. For this case, add the following to the client's `bp.conf` file:

```
VERBOSE
```

and as root on the client execute:

```
touch /usr/openv/netbackup/bpbkar_path_tr
mkdir /usr/openv/netbackup/logs/bpbkar
```

Then retry the operation. The names of the files are logged in the activity log file in the `/usr/openv/netbackup/logs/bpbkar` directory before `bpbkar` processes them. The last file in the log will be the file that is causing problems.

Note Also, use the above procedure for other, "unknown" `bpbkar` hangs.

If the problem is due to mandatory file locking, you can have NetBackup skip the locked files by setting `LOCKED_FILE_ACTION` to `SKIP` in the `/usr/openv/netbackup/bp.conf` file on the client.

- The bpbkar client process is not hung, but due to the files and directories it is scanning, it has not replied to the server within CLIENT_READ_TIMEOUT or CLIENT_CONNECT_TIMEOUT. This has been seen to occur during backups when directories have thousands of unmodified files; it has also been seen when backing up file systems or directories that reside on optical disk, which is considerably slower than magnetic disk.

  For this case, try adding or modifying the CLIENT_READ_TIMEOUT and CLIENT_CONNECT_TIMEOUT values in the server's /usr/openv/netbackup/bp.conf file. The default for the CLIENT_READ_TIMEOUT and CLIENT_CONNECT_TIMEOUT is 300 seconds if unspecified.

Use your system's ps command and monitor CPU utilization to help decide which of the above conditions exist.

When you are through investigating the problem, delete the /usr/openv/netbackup/logs/bpbkar directory, since the log files can become quite large and are not deleted automatically. Also delete /usr/openv/netbackup/bpbkar_path_tr so you do not generate larger log files than needed the next time you create directory /usr/openv/netbackup/logs/bpbkar.

2. On Windows NT/2000 systems, try the following:

   - Disable the following file:

     install_path\Veritas\NetBackup\bin\admincmd\tracker.exe

   - Repair hard drive fragmentation. You could try an application called Diskeeper Lite, which is part of the Windows NT Resource Kit.

   - Make sure there is enough space available in \temp.

3. If the server cannot connect to the client, create bpcd or bpbkar (UNIX and Windows NT/2000 only) activity log directories on the client, retry the operation, and check the resulting logs. If these logs do not provide a clue, create a bpbrm activity log on the server, retry the operation again, and check the resulting activity log.

   If the bpbrm log has entries similar to the following:

```
bpbrm hookup_timeout: timed out waiting during the client hookup
bpbrm Exit: client backup EXIT STATUS 41: network connection timed out
```

   then the problem is in the routing configuration on the server.

   Verify that the client IP address is correct in the name service that is being used. On UNIX, if both NIS and DNS files are used, verify that they match.

   Also, see "Resolving Network Communication Problems" on page 24.

4. If you are using an AIX token ring adapter and the `routed` daemon is running, the timeout can occur because the token ring adapter creates dynamic routes, causing the `routed` daemon to crash.

5. For a FlashBackup client, this can happen if the file system being backed up is very large and has a very large number of files. It can also occur if a large number of concurrent data streams are active at the same time. The corrective action is to add `CLIENT_READ_TIMEOUT` to the `/usr/openv/netbackup/bp.conf` file and set it to increase the timeout interval.

6. Make sure all recommended NetBackup patches have been installed. Check the VERITAS support web site for current patch information. (Go to www.support.veritas.com, then select "NetBackup" followed by "files and updates".)

7. Add the CLIENT_READ_TIMEOUT values to the master server, media server and client when a NetBackup database extension product is installed. The values should all be the same for each server. The value set is dependent on the size of the database being backed up. See the *NetBackup System Administrator's Guide* for more information on CLIENT_READ_TIMEOUT.

Status Code: 42

Message: network read failed

Explanation: An attempt to read data from a socket failed.

Recommended Action:

1. Verify that both the client and the server are operational.

2. Perform "Resolving Network Communication Problems" on page 24.

3. Check the Problems report for clues.

Status Code: 43

Message: unexpected message received

Explanation: The client and server handshaking was not correct.

Recommended Action:

1. Verify that the correct version of software is running on the client and the server.

2. Enable detailed activity logging:
   - On the server, create a `bpbrm` activity log directory.

- On clients, create a `bpcd` activity log directory (created automatically on Macintosh clients).
- Increase the amount of debug information included in the logs as explained in the activity log topics in Chapter 3.

3. Retry the operation and examine the logs.

Note If you are using `bpstart_notify` scripts on UNIX or Windows NT/2000 clients, verify that messages are not being written to stdout or stderr.

Status Code: 44

Message: network write failed

Explanation: An attempt to write data to a socket failed.

Recommended Action:

1. Check the Problems report for information about the error.
2. Verify that the client and servers are operational and connected to the network.
3. Create an activity log directory for the process that reported the problem and the operation. Examine the resulting activity log file for detailed troubleshooting information.
4. Perform "Resolving Network Communication Problems" on page 24.

Status Code: 45

Message: request attempted on a non reserved port

Explanation: An attempt was made to access a client from a nonreserved port.

Recommended Action: Verify that the latest software is installed on the client and server.

- On UNIX NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
- On Windows NT/2000 NetBackup servers, check the *install_path*`\netbackup\version.txt` file or the About NetBackup item on the Help menu.
- On Microsoft Windows clients, check the About NetBackup item on the Help menu.
- On NetWare target clients, check the Version entry in the `bp.ini` file.

- If this is a NetBackup for NetWare client and has a version of NetBackup earlier than 3.0, verify that the client is in a Standard type class.
- On Macintosh clients, check the version file in the bin folder in the NetBackup folder in the Preferences folder.

Status Code: 46

Message: server not allowed access

Explanation: The server is trying to access the client but the server is not listed on the client as a valid server.

Recommended Action: If the server is a valid server, add its name to the client's server list:

- On Windows NT/2000, 98, and 95 clients, add the server on the Servers tab in the Specify NetBackup Machines dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and click Specify NetBackup Machines on the Actions menu.
- On UNIX, and Macintosh clients, add a `SERVER` entry in the `bp.conf` file.
- On NetWare target and OS/2 clients add a `SERVER` entry in the `bp.ini` file.

If you continue to have problems, review "Resolving Network Communication Problems" on page 24 and "Verifying Host Names and Services Entries" on page 32.

Status Code: 47

Message: host is unreachable

Explanation: An attempt to connect to another machine failed.

Recommended Action:

1. Verify that the name service (or services) being used by the client is configured to correctly resolve the host names of the NetBackup server.
2. Verify that the name service (or services) being used by the server is configured to correctly resolve the host name of the NetBackup client.
3. Try to ping the client from the server and the server from the client.
4. If you continue to have problems, perform "Resolving Network Communication Problems" on page 24.

Status Code: 48

Message: client hostname could not be found

Explanation: The system function `gethostbyname()` failed to find the client's host name.

Recommended Action:

1. Verify that the client name is correct in:
   - The NetBackup class configuration on the master server.
   - The General tab in the NetBackup Configuration dialog box and the Clients tab in the Specify NetBackup Machines dialog box (on Microsoft Windows and NetWare nontarget clients). To display these dialog boxes, start the Backup, Archive, and Restore interface on the client. For the General tab, click Configure on the Actions menu; for Clients tab, click Specify NetBackup Machines on the Actions menu.
   - The `bp.conf` file on UNIX and Macintosh clients.
   - The `bp.ini` file on OS/2 and NetWare target clients.
2. On clients and servers, verify that the name service is set up to correctly resolve the NetBackup client names.

   On UNIX clients, verify that the client's host name is in the `/etc/hosts` file or the YP hosts file or NIS maps.

Status Code: 49

Message: client did not start

Explanation: The client failed to start up correctly.

Recommended Action:

1. Verify that software is installed on the client and it is the correct version. If necessary, reinstall the client software.
2. Check for full file systems on the client.
3. Enable detailed activity logging on the client:
   - Create `bpcd` and `bpbkar` (UNIX or Windows NT/2000 only) activity log directories.
   - On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.

- On PC clients, increase the debug or log level as explained in the activity log topics in Chapter 3.

4. Retry the operation and examine the resulting logs.

5. On UNIX systems, use the UNIX `sum` command to check for corrupt binaries.

6. On SGI IRIX 6.2/6.4 systems, clients may be missing the `libdbm.so` shared library. Refer to the SGI/IRIX install CD-ROM for the `eoe.sw.dmi` package.

Status Code: 50

Message: client process aborted

Explanation: The client backup aborted. One instance when this code appears is if a NetBackup master or media server is shut down or rebooted when a backup or restore is in process.

Recommended Action:

1. Enable detailed activity logging:
   - Create a `bpbkar` activity log directory (UNIX or Windows NT/2000 only).
   - Create a `bpcd` activity log directory (this log is created automatically on Macintosh clients.)
   - On UNIX clients, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
   - On PC clients, increase the debug or log level as explained in the activity log topics in Chapter 3.

2. Retry the operation and examine the resulting logs.

3. On UNIX clients, check for core files in the `/` directory.

4. On UNIX clients, check the system log (`/usr/adm/messages` on Solaris) for system problems.

5. This problem can sometimes be due to a corrupt binary.

   On UNIX clients, use the UNIX `sum` command to check the `bpcd`, `bpbkar`, and `tar` binaries, located in `/usr/openv/netbackup/bin` on the client. Reinstall them if they are not the same as in the client directory under `/usr/openv/netbackup/client` on the server.

On a Windows NT/2000 client, check the `bpinetd.exe`, `bpcd.exe`, `bpbkar32.exe`, and `tar32.exe` executables located in the *install_path*`\NetBackup\bin` folder on the client. Reinstall the client if these executables are not the same size as on other Windows NT/2000 clients or are not at the same release level or do not have the same NetBackup patches applied as other Windows NT/2000 clients.

Status Code: 51

Message: timed out waiting for database information

Explanation: The catalog process did not respond within five minutes.

Recommended Action:

1. Verify that the NetBackup Database Manager daemon (service on Windows NT/2000) is running.
2. Verify that there is space in the file system that contains the NetBackup catalogs.
3. Create `bpbrm` and `bpdbm` activity log directories on the server and retry the operation.
4. Look in the activity log files to find more information on the problem.

Status Code: 52

Message: timed out waiting for media manager to mount volume

Explanation: The requested volume was not mounted before the timeout expired. This error can also occur if the volume happens to be a cleaning tape but was not specified as a cleaning tape.

Another possible cause: if the last available drive has a mount request for a non-backup (such as a restore), then a backup requiring the same drive is initiated before the mount completes. This is due to the drive not being reported as busy until the mount completes.

Recommended Action:

1. Verify that the requested volume is available and an appropriate drive is ready and in the UP state.
2. If this occurs during a read operation (restore, duplicate, verify), the drives could be busy. Try increasing the media mount timeout specified by the NetBackup global attribute in order to allow more time for mounting and positioning the media.
3. Verify that the tape is not a cleaning tape that is configured as a regular volume.

4. When the robot is controlled by an Automated Cartridge System, verify that the ACSLS system is up.

5. If this is an initial installation, refer to "To Resolve Common Configuration Problems" on page 13.

6. On Windows NT/2000, check the Event Viewer Application log for error messages that indicate why the tape mount did not complete. On UNIX, check the system log.

Status Code: 53

Message: backup restore manager failed to read the file list

Explanation: The backup and restore manager (`bpbrm`) could not read the list of files to back up or restore.

Recommended Action: Verify that the server software has been installed correctly on all NetBackup servers. If that is not the problem:

1. Create `bpbrm` and `bpsched` activity log directories on the server.

2. On a UNIX NetBackup server, add the `VERBOSE` option to the `bp.conf` file. On a Windows NT/2000 NetBackup server, set the Verbose logging level option on the Universal Settings tab in the Master Server Properties dialog. To display this dialog, see "Using the Configure - NetBackup Window" on page 57.

3. Retry the operation and check the resulting activity logs for detailed troubleshooting information.

Status Code: 54

Message: timed out connecting to client

Explanation: The server could not complete the connection to the client. The accept system call timed out after 60 seconds.

Recommended Action:

1. For a Macintosh or NetWare target client, verify that the server is not trying to connect when a backup or restore is already in progress on the client. These clients can handle only one NetBackup job at a time.

   On a Macintosh, you can check for activity by examining the `NetBackupListen` file in the following folder on the startup disk of the Macintosh client:

   ```
   :System Folder:Preferences:NetBackup:logs:inetd:log.mmddyy
   ```

2. On a Sequent platform, verify that the system has the correct level of TCP/IP.

3. Perform "Resolving Network Communication Problems" on page 24.

4. On UNIX clients, verify that the `/usr/openv/netbackup/bin/bpcd` binary exists and that it is the correct size.

5. Check the `/etc/inetd.conf` file to make sure the `bpcd` path is correct in the following entry:

```
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
```

6. On systems that include NetBackup master, slave, and clients (with NetBackup database extension products installed on one or more clients), make sure the client name is in the master's `/etc/hosts` file.

Status Code: 55

Message: permission denied by client during rcmd

Explanation: The UNIX client does not have the server's name in its `/.rhosts` file.

Recommended Action: Add the server name to the `/.rhosts` file on the UNIX client.

Status Code: 56

Message: client's network is unreachable

Explanation: The server got ENETUNREACH when trying to connect to the client.

Recommended Action: Try to ping the client from the server. Check the IP address for the client. If you still have problems, talk to your network administrator.

Status Code: 57

Message: client connection refused

Explanation: The client refused a connection on the port number for `bpcd`. This can occur because there is no process listening on the `bpcd` port or there are more connections to the `bpcd` port than the network subsystem can handle with the `listen()` call.

Recommended Action:

1. For Windows NT/2000 NetBackup servers:

   a. Make sure the NetBackup client software is installed.

   b. Verify that the `bpcd` and `bprd` port numbers in the `%SystemRoot%\system32\drivers\etc\services` file on the server matches the setting on the client.

c. Verify that the NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog box match the `bpcd` and `bprd` settings in the `services` file. To display this dialog box, start the Backup, Archive, and Restore interface on the server and click Configure on the Actions menu.

The values on the Network tab are written to the `services` file when the NetBackup Client service starts.

d. Verify that the NetBackup client service is running.

e. On Windows NT/2000 systems, for NetBackup 3.0 to NB3.1.1, the *install_path*`\winnt\system32\drivers\etc\services` file may not have correct information. The following entries are correct:

```
bpcd            13782/tcp
bprd            13720/tcp
```

f. Use the following command to see if the master server returns correct information for the client:

install_path`\Veritas\NetBackup\bin\admincmd\bpclntcmd -pn`

2. For UNIX servers:

a. Make sure the NetBackup client software is installed.

b. Verify that the `bpcd` port number on the server (either NIS services map or in `/etc/services`) matches the number in the client's services file.

3. For a Macintosh or NetWare target client, verify that the server is not trying to connect when a backup or restore is already in progress on the client. These clients can handle only one NetBackup job at a time.

4. Perform "Resolving Network Communication Problems" on page 24.

Status Code: 58

Message: can't connect to client

Explanation: The server was unable to connect to the client.

Recommended Action: Perform "Resolving Network Communication Problems" on page 24.

Status Code: 59

Message: access to the client was not allowed

Explanation: The master or media server is trying to access the client, but the server is not recognized by the client as a valid server.

Recommended Action:

1. If the server is a valid server, verify that it is in the server list on the client. If necessary add it as follows:
   - On Windows NT/2000, 98, and 95 clients, add the server on the Servers tab in the Specify NetBackup Machines dialog box. To display this dialog, start the Backup, Archive, and Restore interface on the client and click Specify NetBackup Machines on the Actions menu.
   - On UNIX, and Macintosh clients, add a `SERVER` entry in the `bp.conf` file.
   - On NetWare target and OS/2 clients add a `SERVER` entry in the `bp.ini` file.

   If you change the server list on a UNIX master server, you must stop and then restart the NetBackup Request daemon (`bprd`) and NetBackup database manager daemon (`bpdbm`) for the changes to take effect. On Windows NT/2000, stop and restart the NetBackup Request Manager and NetBackup Database Manager services.

2. On Windows NT/2000 clients, enable `bpinetd` activity logging as follows:

   a. Create a `bpinetd` activity log directory on the client.

   b. Increase the debug or log level as explained in the activity log topics in Chapter 3.

   c. Retry the backup and examine the resulting logs to determine the cause of the failure.

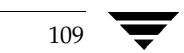
3. On all but Macintosh clients, enable `bpcd` activity logging as follows:

   a. Create a `bpcd` activity log directory on the client.

   b. On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.

   c. On PC clients, increase the debug or log level as explained in the activity log topics in Chapter 3.

   d. Retry the backup and examine the resulting logs to determine the cause of the failure.



4. On Macintosh clients, check the `inetd` and `bpcd` activity logs. Both logs are created automatically.
   - Check the `inetd` log to see if `NetBackupListen` is running.
   - Check the `bpbkar` and `tar` messages in the `bpcd` log file.

     To increase the amount of information included in the logs, set the `loglevel` parameter in the `mac.conf` file to a higher value.

5. Check the `bpcd` activity log to determine the server's peername and what comparisons are being made.

   The `bpcd` process compares NetBackup server list entries to the peername of the server attempting the connection and rejects the connection if the names are different. If necessary, change the server list entry on the client to match the peername.

6. On Windows NT/2000 clients, check the following:
   - Verify that NetBackup for Windows NT/2000 software was installed under a Windows NT/2000 administrator account.

     If NetBackup is under another type of account, reinstall it under an administrator account. The installation will complete successfully under a non-administrator account but the NetBackup Client service is not added to Windows NT/2000 and the NetBackup server cannot access the client.
   - Verify that the Windows NT/2000 TCP/IP service specifies the domain server that resolves names for the subnet that contains the NetBackup servers.

     UNIX and Windows NT/2000 clients are frequently not on the same subnet and use different domain servers. When this condition exists the NetBackup servers and Windows NT/2000 clients may be able to ping one another, but the server is still unable to access the Windows NT/2000 client.

7. If the preceding steps do not resolve this problem, see "Resolving Network Communication Problems" on page 24.

8. If NetBackup is using multiple network interfaces with slave servers, make sure the interface names appear in the client's `/usr/openv/netbackup/bp.conf` file.

Status Code: 60

Message: client cannot read the mount table

Explanation: The backup process on the client could not read the list of mounted file systems.

Recommended Action:

1. Execute a `df` to see if the system can read the mount table.

2. On an SCO system, code 60 can occur because the mount-point path name exceeds 31 characters, which is the maximum allowed on an SCO system. The `bpbkar` activity log on the client will show a message similar to the following:

   ```
   bpbkar build_nfs_list: FTL - cannot statfs net Errno: 42406
   ```

   To eliminate these errors for future backups, create a mount point with a shorter name and symbolically link the long name to the short name.

3. For detailed troubleshooting information, create a `bpbkar` activity log directory, retry the operation, and examine the resulting log.

Status Code: 61

Message: wbak was killed

Explanation: The `wbak` process on the Apollo was killed.

Recommended Action: Try the backup again.

Status Code: 62

Message: wbak exited abnormally

Explanation: The `wbak` process on the Apollo exited abnormally.

Recommended Action: Try running `wbak` by hand to determine the source of the problem. Direct the output of the `wbak` command to `/dev/null` to avoid filling up your file system and use the following parameters:

`-l -nhi -pdtu -stdout -nwla and -full or -af` *date*

Status Code: 63

Message: process was killed by a signal

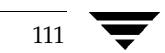
Explanation: A kill signal was sent to the client process.

Recommended Action: This is usually caused by someone intentionally terminating a backup.

Status Code: 64

Message: timed out waiting for the client backup to start

Explanation: The client did not send a ready message to the server within the allotted time.



Recommended Action:

1. On all but Macintosh clients, enable `bpcd` activity logging as follows:
   a. Create a `bpcd` activity log directory on the client.
   b. On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
   c. On PC clients, increase the debug or log level as explained in the activity log topics in Chapter 3.
2. On Macintosh clients, check the `inetd` and `bpcd` activity logs. Both logs are created automatically.
   - Check the `inetd` log to see if `NetBackupListen` is running.
   - Check the `bpbkar` and `tar` messages in the `bpcd` log file.

     To increase the logging level, set the `loglevel` parameter in the `mac.conf` file to a higher value.
3. On a UNIX or Windows NT/2000 client, create the `bpbkar` activity log directory on the client.
4. On Windows NT/2000 clients, verify that the NetBackup Client service is running.
5. On a UNIX client, use the `ps` command to check for a client process that is using too much CPU time.
6. Retry the backup and examine the activity logs for clues on the cause of the failure.

Status Code: 65

Message: client timed out waiting for the continue message from the media manager.

Explanation: The tape manager, `bptm` reported that the media did not load and position within the allotted time.

Recommended Action: Verify that the requested volume is available and the required device is in an UP state.

For detailed debug information:

1. Create a bptm activity log directory on the server.

2. On a UNIX NetBackup server, add the VERBOSE option to the bp.conf file. On a Windows NT/2000 NetBackup server, set the Verbose logging level option on the Universal Settings tab in the Master Server Properties dialog (see "Using the Configure - NetBackup Window" on page 57).

3. Retry the operation and check the bptm activity log file for information on the drive, robot, and tape that is causing the timeout.

4. On a Windows NT/2000 NetBackup server (master or media), check the Event Viewer Application log for error messages that indicate why the tape mount did not complete.

Status Code: 66

Message: client backup failed to receive the CONTINUE BACKUP message

Explanation: The client bpbkar process did not receive the message from the server that indicates that the server is ready to continue.

Recommended Action: Verify that the server did not crash. If that is not the problem and you need more information:

1. On UNIX and Windows NT/2000 clients, enable bpbkar activity logging.

   a. Create a bpbkar activity log directory.

   b. On a UNIX client, add the VERBOSE option to the bp.conf file. On a Windows NT/2000 client, set Verbose on the TroubleShooting tab in the NetBackup Configuration dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and click Configure on the Actions menu.

2. On other PC clients except Macintosh, create an activity log directory for bpcd (the bpcd log is created automatically on Macintosh).

   To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

3. On the master server create bpsched and bpbrm activity log directories. If there are media servers involved, create a bpbrm activity log directory on them.

4. Retry the operation and check the resulting activity logs.

Status Code: 67

Message: client backup failed to read the file list

Explanation: The client could not read the list of files to back up.

Recommended Action: First, verify that the server did not crash. If that is not the problem and you need more information:

1. Set up activity logging:

   a. On the server, create a `bpbrm` activity log directory.

   b. On UNIX and Windows NT/2000 clients, create a `bpbkar` activity log directory.

   c. On other PC clients except Macintosh, create an activity log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

   To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

2. Retry the operation and check the resulting activity logs.

Status Code: 68

Message: client timed out waiting for the file list

Explanation: The client did not receive the list of files to back up within the allotted time. This list comes from the server.

Recommended Action: First, verify that the server did not crash. If that is not the problem and you need more information:

1. Set up activity logging:

   a. On the server, create an activity log directory for `bpbrm`.

   b. On UNIX and Windows NT/2000 clients, create a `bpbkar` activity log directory.

   c. On other PC clients except Macintosh, create an activity log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

   To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

2. Retry the operation and check the resulting activity logs.

Status Code: 69

Message: invalid file list specification

Explanation: The file list received from the server had invalid entries.

Recommended Action: Check the class file list. If wildcards are used, verify there are matching bracket characters ([and]). If the file list contains UNC (Universal Naming Convention) names, ensure they are properly formatted.

Status Code: 70

Message: an entry in the file list expanded to too many characters

Explanation: The wildcards used in one of the file list entries caused too many files to be specified.

Recommended Action: Change the wildcards in the file list to specify fewer files.

Status Code: 71

Message: none of the files in the file list exist

Explanation: The files in the file list did not match any of the files on the client. This error can occur when there is only one file in the file list and the file cannot be backed up due to an I/O error.

Recommended Action:

1. Verify that the correct file list is specified for this client.
2. On Windows NT/2000 clients, verify that the account used to start the NetBackup Client service has read access to the files.

   If you are backing up a network drive or a UNC (universal naming convention) path, use the Services application in the Windows NT/2000 Control Panel to verify that the NetBackup Client service does not start under the SYSTEM account. The SYSTEM account cannot access network drives.

   To back up network drives or UNC paths, change the NetBackup Client service startup to log in as a user that has permission to access network drives.
3. Check the All Log Entries report for clues.
4. Set up activity logging:
   - On UNIX and Windows NT/2000 clients, create an activity log directory for `bpbkar`.

- On other PC clients except Macintosh, create an activity log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

5. Retry the operation and check the resulting activity logs.

6. On Novell systems, check the following:

   - For the nontarget version of NetBackup for NetWare, the backup class type must be "NetWare", and the files list should include a forward slash (/) only. There should be nothing else in the files list.

     To check the class type and files list, start Backup Policy Management and right-click the name of a class. Click the Attributes tab to check the class type; click the Files tab to check the contents of the files list.

   - For the target version, the backup class type must be "Standard", and the class files list must be formatted as follows:

     /*target_name*

     where a forward slash precedes the variable *target_name*.

     To check the class type and files list, start Backup Policy Management and right-click the name of a class. Click the Attributes tab to check the class type; click the Files tab to check the contents of the files list.

Note For the target version, the following NetWare message may be another indicator of incorrect class type (this message would appear in the Novell client's bpcd log):

```
unable to connect to service, scheduled access not specified
```

Make sure the class type is set to "Standard".

Status Code: 72

Message: the client type is incorrect in the configuration database

Explanation: The class type attribute in the class configuration indicates that the client is one type, but the installed software is for another type.

Recommended Action: Verify that the class type attribute for the class is correct. Also, for UNIX, do not place Apollo and standard clients in the same class.

Status Code: 73

Message: bpstart_notify failed

Explanation: The `bpstart_notify` script returned a nonzero exit code.

Recommended Action: Check the `bpstart_notify` script on the client to see if it performs as desired.

Status Code: 74

Message: client timed out waiting for bpstart_notify to complete

Explanation: The `bpstart_notify` script on the client took too long.

Recommended Action: Try to speed up the `bpstart_notify` script or set the `BPSTART_TIMEOUT` on the server to a value that is larger than the default.Set `BPSTART_TIMEOUT` in the `bp.conf` file on a UNIX NetBackup server. On a Windows NT/2000 NetBackup server, use the Configure - NetBackup window to set Backup Start Notify Timeout (see "Using the Configure - NetBackup Window" on page 57).

Status Code: 75

Message: client timed out waiting for bpend_notify to complete

Explanation: The `bpend_notify` script on the client took too long.

Recommended Action: Try to speed up the `bpend_notify` script or set `BPEND_TIMEOUT` on the server to a value that is larger than the default. Set `BPEND_TIMEOUT` in the `bp.conf` file on a UNIX NetBackup server. On a Windows NT/2000 NetBackup server, use the Configure - NetBackup window to set Backup End Notify Timeout.

Status Code: 77

Message: execution of the specified system command returned a nonzero status

Explanation: An immediate command returned a nonzero status.

Recommended Action:

1. Verify that the command is specified correctly.
2. Execute the command manually to see if the desired result is produced.
3. For detailed troubleshooting information, set up activity logging:
   a. On UNIX and Windows NT/2000 clients, create an activity log directory for `bpbkar`.
   b. On other PC clients except Macintosh, create an activity log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

c. Retry the operation and check the resulting activity log.

Status Code: 78

Message: afs/dfs command failed

Explanation: Indicates an AFS `vos` command failure.

Recommended Action:

1. Check the NetBackup Problems Report for additional information on why the command failed.

2. The `bpbkar` activity log shows the command that was executed. Create an activity log directory for `bpbkar`. Retry the operation and retry the resulting activity log.

3. Try executing the `vos` command manually to duplicate the problem.

Status Code: 80

Message: Media Manager device daemon (`ltid`) is not active

Explanation: If the server is UNIX, the Media Manager device daemon, `ltid`, is not running. If the server is Windows NT/2000, the NetBackup Device Manager service is not running.

Recommended Action:

1. On Windows NT/2000, use the Activity Monitor or the Services application in the Windows NT/2000 Control Panel to see if the NetBackup Device Manager service is running. If it is not running, start it. To enable verbose logging, place `VERBOSE` on a line by itself in the *install_path*`\Volmgr\vm.conf` file before starting the service.

2. On UNIX, use `vmps` to see if `ltid` is running and if necessary start it in verbose mode with the following command:

   ```
   /usr/openv/volmgr/bin/ltid -v
   ```

   Or, add a `VERBOSE` entry to the Media Manager configuration file, `/usr/openv/volmgr/vm.conf`. Create the `vm.conf` file if necessary.

3. On UNIX, check the system logs to verify that `ltid` starts.

Note ltid or the NetBackup Device Manager service is used only if devices are attached to the system.

Status Code: 81

Message: Media Manager volume daemon (vmd) is not active

Explanation: The tape manager (bptm) could not communicate with the NetBackup Volume Manager service (Windows NT/2000) or the Media Manager volume daemon (UNIX). This communication is required for most operations.

Recommended Action: On UNIX, verify that the Media Manager device daemon (ltid) and the volume daemon (vmd) are running. Start them if necessary.

On Windows NT/2000, verify that both the NetBackup Device Manager service and the NetBackup Volume Manager service are running. Start them if necessary.

Note ltid or the NetBackup Device Manager service is used only if devices are attached to the system.

Status Code: 82

Message: media manager killed by signal

Explanation: The tape manager (bptm) or disk manager (bpdm) was terminated by another process or a user.

Recommended Action: This should not occur in normal operation. If you want to terminate an active backup, use the NetBackup Activity Monitor.

When backing up a DomainOS client (for example, Apollo), this has been seen to occur after the server has not received anything on the socket for at least 300 seconds, thus causing a client read timeout and breaking the connection. The bpbkar activity log had an entry similar to the following:

```
13:22:49 [1347] <16> bpbkar: ERR - Extra output - - ECONNRESET
Connection reset by peer (UNIX/errno status)
```

Increasing the CLIENT_READ_TIMEOUT value (in this instance to 900) has resolved this problem.

Status Code: 83

Message: media open error

Explanation: The tape manager (bptm) or disk manager (bpdm) could not open the device or file that the backup or restore must use.

Recommended Action:

1. For additional information, check the following:
   - NetBackup Problems report
   - System log (UNIX)
   - Event Viewer Application log (Windows NT/2000)
2. Typically, this status code indicates a drive configuration problem that allows more than one process at a time to open the device.

   On UNIX, the problem could be due to:
   - Two (or more) devices were configured that are really the same physical device (for different densities perhaps). Verify that none of the `/dev` files used for these devices have the same major or minor numbers.
   - Links exist in the file system that are allowing users access to the drives.
   - The configuration for the drives was modified (in the administrator interface or `vm.conf`) and the Media Manager device daemon, `ltid`, was not restarted. Verify the configuration and start `ltid`.

   On Windows NT/2000, the problem could be that the Media Manager device configuration was modified but the NetBackup Device Manager service was not restarted. Verify the configuration and restart the NetBackup Device Manager service.
3. Make sure the tapes are not write protected.
4. For detailed troubleshooting information:
   a. Create an activity log directory for `bpdm` (if the device is disk) or `bptm` (if the device is tape).
   b. On UNIX, restart `ltid` in the verbose mode by executing:

      ```
      /usr/openv/volmgr/bin/ltid -v
      ```

      Or, add a `VERBOSE` entry to the Media Manager configuration file, `/usr/openv/volmgr/vm.conf`. Create the `vm.conf` file if necessary.
   c. On Windows NT/2000, enable verbose logging by adding `VERBOSE` on a line by itself in the *install_path*`\Volmgr\vm.conf` file. Then, stop and restart the NetBackup Device Manager service.
   d. Retry the operation and check the resulting activity log files.

e. On UNIX systems, look at the `/usr/openv/netbackup/db/media/errors` log (which is also included in the `/usr/openv/netbackup/bin/goodies/support` script output) for a drive that is frequently producing errors.

Status Code: 84

Message: media write error

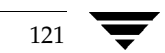
Explanation: The system's device driver returned an I/O error while NetBackup was writing to removable media or a disk file.

Recommended Action:

1. For additional information, check the following:
   - NetBackup Problems report to determine the device or media that caused the error
   - System and error logs for the system (UNIX)
   - Event Viewer Application and System logs (Windows NT/2000)
2. If NetBackup was writing backups to a disk file, verify that the disk has enough space for the backup.

   For a catalog backup to a disk path on a UNIX system, you may be trying to write a image greater than two gigabytes. File sizes greater than two gigabytes is a limitation on many UNIX file systems. Tape files do not have this limit.
3. If the media is tape or optical disk, check for:
   - A defective or dirty drive, in which case, clean it or have it repaired (refer to the `tpclean` command for robotic drives).
   - The wrong media type. Verify that the media matches the drive type you are using. On an optical drive, the platters may not be formatted correctly.
   - Defective media. If this is the case, use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.
   - Incorrect drive configuration. Verify the Media Manager and system configuration for the drive.

     For example, on UNIX the drive could be configured for fixed mode when it must be variable mode. See the *Media Manager Device Configuration Guide* for more information.



Status Code: 85

Message: media read error

Explanation: The system device driver returned an I/O error while NetBackup was reading from tape, optical disk, or a disk file.

Recommended Action:

1. For additional information, check the following:
   - NetBackup Problems report to determine the device or media that caused the error
   - System and error logs for the system (UNIX)
   - Event Viewer Application and System logs (Windows NT/2000)
2. Check for the following:
   - A defective or dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
   - Incorrect drive configuration. Verify the Media Manager and system configuration for the drive.

     For example, on UNIX the drive could be configured for fixed mode when it must be variable mode. See the *Media Manager Device Configuration Guide* for more information.
   - Defective media. In this case, you may not be able to recover all the data on the media. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.
   - The wrong media type. Verify that the media matches the drive type you are using.

Status Code: 86

Message: media position error

Explanation: The system's device driver returned an I/O error while NetBackup was positioning media (tape or optical disk).

Recommended Action:

1. For additional information, check the following:
   - NetBackup Problems report to determine the device or media that caused the error
   - System and error logs for the system (UNIX)

- Event Viewer Application and System logs (Windows NT/2000)

2. Check for the following:
   - A defective or dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
   - Incorrect drive configuration. Verify the Media Manager and system configuration for the drive.

     For example, on UNIX the drive could be configured for fixed mode when it must be variable mode. See the *Media Manager Device Configuration Guide* for more information.
   - Defective media. In this case, some data may be lost. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.
   - The wrong media type. Verify that the media matches the drive type you are using.

Status Code: 87

Message: media close error

Explanation: The system's device driver returned an I/O error while NetBackup was closing a tape or optical disk.

Recommended Action:

1. For additional information, check the following:
   - NetBackup Problems report to determine the device or media that caused the error
   - System and error logs for the system (UNIX)
   - Event Viewer Application and System logs (Windows NT/2000)
2. Check for the following:
   - A defective or dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
   - Defective media. In this case, some data may be lost. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.

Status Code: 88

Message: Auspex SP/Backup failure

Explanation: NetBackup detected a problem when backing up an Auspex FastBackup client.

Recommended Action: Check the All Log Entries report. If more details are required, create `bptm` and `bpbrm` activity log directories on the server. Then, retry the operation and check the resulting log files. This error is usually due to a configuration problem.

Status Code: 90

Message: media manager received no data for backup image

Explanation: The tape manager (`bptm`) or disk manager (`bpdm`) received no data when performing a backup or archive. This can occur for incremental backups where no data was backed up because no files have changed.

Recommended Action:

1. For additional information, check the following:
   - NetBackup Problems report to determine the device or media that caused the error
   - System and error logs for the system (UNIX)
   - Event Viewer Application log (Windows NT/2000)
2. Verify the Media Manager and system configuration for the drive.

   For example, on UNIX the drive may not be set for variable mode in a case where that mode is required by NetBackup. Check the *Media Manager Device Configuration Guide* for drive configuration information.
3. Verify that the Media Manager configuration for the backup device matches what is specified for the storage unit in the NetBackup class.
4. Verify that you are using the correct media in the drive.
5. For detailed debug information, create a `bpdm` or `bptm` activity log directory (whichever applies) on the server. If the client is Windows NT/2000, also create a `bpbkar` activity log directory on the client. Retry the operation and check the resulting activity logs. Retry the operation. Check the resulting activity log file.

Status Code: 91

Message: fatal NB media database error

Explanation: The tape manager (`bptm`) received an error while reading or updating its media catalog.

Recommended Action:

1. Check the All Log Entries report for more information.
2. Check the NetBackup Media Lists report to see if the catalog is intact. If the catalog is not intact, consider reloading it from the latest NetBackup catalog backup volume.
3. Verify that the disk partition on which the catalog resides has enough space.
4. If the above actions do not explain the problem, check the NetBackup Problems report.
5. For detailed troubleshooting information, create a `bptm` activity log directory on the server and retry the operation. Check the resulting activity log file.
6. Contact customer support and send appropriate problem and activity log sections.

Status Code: 92

Message: media manager detected image that was not in tar format

Explanation: When performing a restore, the tape manager (`bptm`) or disk manager (`bpdm`) could not find a `tar` header at the offset it expected.

Recommended Action:

1. Perform a `bpverify` of the affected image to determine if it is written correctly.
2. Check the NetBackup Problems report for additional information about the error.
3. Verify the Media Manager and system configuration for the drive.

   For example, on some UNIX systems, for example, if you do not configure the drive for variable-mode block size writes, backup images written to the media produce this error when an attempt is made to restore the image. For example, you see the following sequence of events:

   - Backup succeeds
   - Verify succeeds
   - Restore fails

   The `bptm` activity log shows an error similar to

```
00:58:54 [2304] <16> write_data: write of 32768 bytes indicated
                     only 29696 bytes were written, errno = 0
```

In this case, configure the drive for variable-mode block sizes and suspend media written on that device. See the *NetBackup Device Configuration Guide*.

The images written to those media may be restorable (this is platform dependent), but single file restores are almost guaranteed to fail. You can choose to expire these media and regenerate the backups, or you can attempt to duplicate the images on these media to another device and then expire the original copy.

4. Error code 92 has been encountered on some relabeled and value-added 8-mm tape drives where the drive's microcode incorrectly processes a "forward space record" SCSI command.

5. If the problem is not one of the above, create an activity log directory for either `bpdm` or `bptm` and retry the operation. Check the resulting activity log file.

Status Code: 93

Message: media manager found wrong tape in drive

Explanation: When loading a volume for a backup or restore, the tape manager (`bptm`) found a volume loaded that did not have the expected tape header. This can indicate that volumes in a robot are not in the slots indicated in the Media Manager volume configuration.

Recommended Action:

- If the volume is in a robot and the robot supports barcodes, perform a Compare Contents with Volume Configuration (Verify Robot Contents on UNIX). The resulting report shows which media ID was found and validates its slot number with what is in the Media Manager volume configuration. Then, either change the physical location in the robot or change the volume configuration to show the correct slot.
- If the volume was mounted on a nonrobotic drive, verify that the correct volume was mounted and assigned.

Status Code: 94

Message: cannot position to correct image

Explanation: When searching for a backup image to restore, the tape manager (`bptm`) did not find the correct backup ID at the expected position on the volume. This can indicate a drive hardware problem.

Recommended Action:

1. Try the restore on another drive if possible.

2. For additional information, check the following:

- NetBackup Problems report to determine the device or volume that caused the error
- System and error logs for the system
- Event Viewer Application and System logs (Windows NT/2000)

3. For detailed troubleshooting information, create an activity log directory for `bptm` and retry the operation. Check the resulting activity log files.

Status Code: 95

Message: requested media id not found in NB media database and/or MM volume database

Explanation: An operation was requested on a media ID for which NetBackup does not have a record. An example of this is using `bpmedia` to suspend or freeze a media ID that does not exist.

Recommended Action: Run a NetBackup Media List report to determine the valid media IDs. Then, retry the command with a valid media ID.

Status Code: 96

Message: unable to allocate new media for backup, storage unit has none available

Explanation: The tape manager (`bptm`) could not allocate a new volume for backups. This indicates that the storage unit has no more volumes available in the volume pool for this backup.

Recommended Action: Check the NetBackup Problems report to determine the storage unit that is out of media.

1. If the storage unit is a robot and there are empty slots, add more volumes (remember to specify the correct volume pool).
   - If there are no empty slots, move some media to nonrobotic and then add new volumes.
   - If you are having difficulty keeping track of your available volumes, try the `available_media` script:

     On UNIX, this script is in:

     `/usr/openv/netbackup/bin/goodies/available_media`

     On Windows NT/2000, the script is in:

     install_path`\NetBackup\bin\goodies\available_media.cmd`

This script lists all volumes in the Media Manager volume configuration, and augments that list with information on the volumes currently assigned to NetBackup.

2. If the storage unit and volume pool appear to have media, verify the following:
   - Volume is not FROZEN or SUSPENDED.

     Check for this condition by using the NetBackup Media List report. If the volume is frozen or suspended, use the `bpmedia` command to unfreeze or unsuspend it (if that is desired).
   - Volume has not expired or exceeded its maximum number of mounts.
   - Volume Database Host name for the device is correct.

     If you change the Volume Database Host name, stop and restart the Media Manager device daemon, `ltid`, (if the server is UNIX) or the NetBackup Device Manager service (if the server is a Windows NT/2000 system).
   - The correct host is specified for the storage unit in the NetBackup configuration.

     The host connection should be the server (master or media) that has drives connected to it.
   - The Media Manager volume configuration has media in the correct volume pool and unassigned or active media is available at the required retention level.

     Use the NetBackup Media List report to show the retention levels, volume pools, and status (active and so on) for all volumes. Use the NetBackup Media Summary report to check for active volumes at the correct retention levels.
3. In some configurations, the NetBackup `bptm` process is rejected when requesting media from the `vmd` process (NetBackup Volume Manager service on Windows NT/2000) because that process cannot determine the name of the host that is making the request.

   This can be due to incorrect network configuration involving:
   - Multiple network interfaces
   - `/etc/resolv.conf` on those UNIX systems that use it
   - Running DNS and not having reverse addressing configured
4. Create `bptm` and `vmd` activity log directories and retry the operation.
5. Examine the `bptm` activity log to verify that `bptm` is connecting to the correct system. If an error is logged, examine the `vmd` log.

   On UNIX, the `vmd` log is:

/usr/openv/volmgr/debug/daemon/log.xxxxxx

On Windows NT/2000, the vmd log is:

install_path\Volmgr\debug\daemon\xxxxxx.log

6. If this is a new storage unit, and this is the first attempt to use it, stop and restart NetBackup on the master server.

Note The bptm activity logs (in verbose mode) usually show the NetBackup media selection process.

Status Code: 97

Message: requested media id is in use, cannot process request

Explanation: An operation was requested on a media ID that is in use. An example of this is attempting to suspend or freeze a volume while it is being used for a backup or restore.

Recommended Action: Retry the command when the volume is not in use. Use the Device Monitor to determine if the volume is in use (on UNIX you can also use xdevadm).

Status Code: 98

Message: error requesting media (tpreq)

Explanation: The tape manager and optical manager (bptm) received an error when requesting a media mount from the NetBackup Device Manager service on Windows NT/2000 or the Media Manager device daemon (ltid) on UNIX.

Recommended Action: Check the NetBackup Problems report to determine the reason for the failure. The most common cause is that the NetBackup Device Manager service on Windows NT/2000 or the Media Manager device daemon (ltid) on UNIX is not running. Start it if necessary.

Status Code: 99

Message: NDMP backup failure

Explanation: None of the paths in your NDMP class file list was backed up successfully.

Recommended Action: Check the NetBackup All Log Entries report for more information. A possible cause for this error is that none of the backup paths exist on the NDMP host.

Status Code: 100

Message: system error occurred while processing user command

Explanation: A system call failed in `bparchive`, `bpbackup`, `bplist`, or `bprestore`.

Recommended Action:

1. Enable activity logging for `bparchive`, `bpbackup`, `bplist`, or `bprestore` (as appropriate) by creating activity log directories for them.

   On UNIX, if a nonroot user is having problems, verify that the directory created has mode 666. Look for and correct any reported errors.

2. Retry the operation and check the resulting logs.

   If the logs do not reveal the problem, use the command line version of the command and correct any problems that are reported on stderr.

Status Code: 101

Message: failed opening mail pipe

Explanation: The process that attempts to send mail could not open the pipe to the server.

Recommended Action: Verify that mail is configured on the client. For detailed troubleshooting information, create a `bpcd` activity log directory and retry the operation. Check the resulting `bpcd` activity log.

Status Code: 102

Message: failed closing mail pipe

Explanation: The process that sends mail could not close the pipe to the server.

Recommended Action: Verify that mail is configured on the client. For detailed troubleshooting information, create a `bpcd` activity log directory and retry the operation. Check the resulting `bpcd` activity log.

Status Code: 105

Message: file pathname exceeds the maximum length allowed

Explanation: The path name built by using the current working directory exceeds the maximum path length allowed by the system.

Recommended Action: Shorten the current working directory path length.

Status Code: 106

Message: invalid file pathname found, cannot process request

Explanation: One of the file paths to be backed up or archived is not valid.

Recommended Action: Verify that full path names are used (they start with / on UNIX), and they are less than the maximum path length for the system. Also, verify that the files exist and the permissions allow NetBackup to access them.

Status Code: 110

Message: Cannot find the NetBackup configuration information

Explanation: On Windows NT/2000, NetBackup could not read the registry entries that were created during installation. On UNIX, the `/usr/openv/netbackup/bp.conf` file does not exist.

Recommended Action: On Windows NT/2000, reinstall NetBackup software on the client. On UNIX, create a `/usr/openv/netbackup/bp.conf` file with at least the following lines:

`SERVER =` *server_name*
`CLIENT_NAME =` *client_name*

Status Code: 111

Message: No entry was found in the server list

Explanation: On UNIX, the `SERVER =` *server_name* line is missing in the `bp.conf` file. On Windows NT/2000, the server list contains no entries.

Recommended Action:

- On a UNIX client, add the following line to the top of the `/usr/openv/netbackup/bp.conf` file:

  `SERVER =` *server_name*

- On a Microsoft Windows or nontarget NetWare client, add the server name on the Servers tab in the Specify NetBackup Machines dialog box. To display this dialog, start the Backup, Archive, and Restore interface on the client and click Specify NetBackup Machines on the Actions menu.
- On an OS/2 or NetWare target client, add the server name to the `bp.ini` file.
- On a Macintosh client, add the `SERVER =` *server_name* line to the `bp.conf` file in the NetBackup folder in the Preferences folder.

Status Code: 112

Message: no files specified in the file list

Explanation: A restore was requested with no files in the file list.

Recommended Action: Specify at least one file to be restored.

Status Code: 120

Message: cannot find configuration database record for requested NB database backup

Explanation: The program that backs up the NetBackup internal catalogs could not find the attributes that indicate which media IDs to use or paths to back up. This error should not occur under normal circumstances.

Recommended Action:

1. Check the NetBackup Problems report for additional information about the error.
2. For detailed troubleshooting information, create `admin` and `bpdbm` activity log directories and retry the operation. Check the resulting activity logs.
3. Contact customer support and send appropriate problem and activity log sections detailing the error.

Status Code: 121

Message: no media is defined for the requested NB database backup

Explanation: NetBackup attempted to back up its internal catalogs and there were no media IDs defined in the catalog backup configuration.

Recommended Action: Add the media IDs to the catalog backup configuration. Verify that the media IDs are in the NetBackup volume pool.

Status Code: 122

Message: specified device path does not exist

Explanation: The NetBackup internal catalogs were backed up by using the `bpbackupdb` command line and specifying a raw device file that does not exist.

Recommended Action: Retry the command using a valid device file name.

Status Code: 123

Message: specified disk path is not a directory

Explanation: NetBackup attempted to back up its internal catalogs and the backup attributes were set to dump to a disk. However, the disk file path already exists and is not a directory.

Recommended Action: Specify a different disk path for the catalog backup or delete the file that already exists.

Status Code: 124

Message: NB database backup failed, a path was not found or is inaccessible

Explanation: One or more of the paths specified in the catalog backup configuration could not be backed up.

Recommended Action:

1. Check the NetBackup Problems report for additional information about the error. Some possible causes are:
   - The path does not exist.
   - On a UNIX system, there is a symbolic link in one of the paths.
2. After determining which path could not be accessed, correct the path names in the catalog backup configuration.

Status Code: 125

Message: another NB database backup is already in progress

Explanation: Only one NetBackup catalog backup may be active at any given time.

Recommended Action: None.

Status Code: 126

Message: NB database backup header is too large, too many paths specified

Explanation: Too many paths were specified in the NetBackup catalog backup configuration to fit in a fixed-size media header. This error should not occur under normal circumstances.

Recommended Action: Delete some of the paths from the catalog backup configuration.

Status Code: 127

Message: specified media or path does not have a valid NB database backup header

Explanation: The `bprecover` command was issued and the media ID specified does not have valid catalog backup data.

Recommended Action: Validate that the correct media ID is being used.

Status Code: 130

Message: system error occurred

Explanation: An error occurred that prevents the product from operating in a consistent fashion. This error is usually related to a system call.

Recommended Action:

1. Check the NetBackup Problems report for additional information about the error.
2. Check the system log for reported problems.
3. For detailed troubleshooting information, create `bpdbm`, `bpsched`, `bptm`, and `bprd` activity log directories on the master server and retry the operation. Check the resulting activity logs.

Status Code: 131

Message: client is not validated to use the server

Explanation: The client name, as determined from the connection to the server, did not match any client name in the NetBackup configuration and there was no `altnames` configuration for this client on the master server. A client and server that have multiple network connections can encounter this problem if the name by which the client is configured is not the one by which its routing tables direct connections to the server.

Recommended Action:

1. Examine the NetBackup Problems report.
2. Create an activity log directory for `bprd` and retry the operation. Check the resulting activity log to determine the connection and client names.

   Depending on the request type (restore, backup, and so on.), you may need or want to:

   - Change the client's configured name.
   - Modify the routing tables on the client.
   - On the master server, set up an `altnames` directory and file for this client (see the *NetBackup System Administrator's Guide - UNIX*).

     or

   - On a UNIX master server, create a soft link in the NetBackup image catalog.
3. Review "Verifying Host Names and Services Entries" on page 32.

Status Code: 133

Message: invalid request

Explanation: One of two explanations exist.

- A request was made that is unrecognized. This usually results from different versions of NetBackup software being used together.
- If a client receives this error in response to a list or restore request, it means that the `DISALLOW_CLIENT_LIST_RESTORE` or `DISALLOW_CLIENT_RESTORE` option exists in the `bp.conf` file on a UNIX NetBackup server or registry on a Windows NT/2000 NetBackup server. These options deny list and restore requests from all NetBackup clients.

Recommended Action:

1. If you suspect that the software versions are the problem, verify that all NetBackup software is at the same version level.
   - On UNIX NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
   - On Windows NT/2000 NetBackup servers, check the *install_path*`\netbackup\version.txt` file or the About NetBackup item on the Help menu.
   - On Microsoft Windows clients, check the About NetBackup item on the Help menu.
   - On NetWare target clients, check the Version entry in the `bp.ini` file.

     If the client software is earlier than 3.0, verify that the client is in a Standard type class.
   - On Macintosh clients, check the version file in the bin folder in the NetBackup folder in the Preferences folder.
2. If the server is denying list and restore requests, remove the `DISALLOW_CLIENT_LIST_RESTORE` and `DISALLOW_CLIENT_RESTORE` options from the `bp.conf` file on a UNIX NetBackup server or registry on a Windows NT/2000 NetBackup server. Then, stop and restart the NetBackup request daemon (UNIX) or NetBackup Request Manager service (Windows NT/2000).
3. For detailed troubleshooting information, create `bpdbm`, `bprd`, and `admin` activity log directories. Then, retry the operation and check the resulting activity logs.

Status Code: 135

Message: client is not validated to perform the requested operation

Explanation: This is usually caused by a request to restore files to a client other than the one that made the request and the request did not come from the root user (administrator on Windows NT/2000) on a NetBackup server.

Recommended Action: Retry the operation as a root user (administrator on Windows NT/2000) on the master server. Also see status code 131.

Status Code: 140

Message: user id was not superuser

Explanation: The process was started by a user or process that did not have root privileges (on UNIX) or administrator privileges (on Windows NT/2000).

Recommended Action: If desired, give the user or process administrator privileges (on Windows NT/2000) or root privileges (on UNIX) and retry the operation.

Status Code: 141

Message: file path specified is not absolute

Explanation: The file specification must be an absolute path.

Recommended Action: Correct the file specification and retry the command.

Status Code: 142

Message: file does not exist

Explanation: This code is reserved for future use.

Recommended Action: None.

Status Code: 143

Message: invalid command protocol

Explanation: An ill-formed request was made to the NetBackup request daemon (UNIX) or Request Manager service (Windows NT/2000). This can be due to mismatched versions of the product, corrupted network communication, or to a non-NetBackup process sending data across the port for the daemon or service.

Recommended Action: Examine the NetBackup error logs to determine the system that was the source of the data and on that system determine the process that initiated the request. If it was a NetBackup process, verify that the process or command is compatible with the version of software on the server.

Status Code: 144

Message: invalid command usage

Explanation: This status code is due to a NetBackup process being started with improper options or an incompatibility in the product.

Recommended Action: Either correct the command or verify that all NetBackup binaries are at the same version level.

Status Code: 145

Message: daemon is already running

Explanation: There is another copy of the process executing.

Recommended Action: Terminate the current copy of the process and then restart the process.

Status Code: 146

Message: cannot get a bound socket

Explanation: The daemon (service on Windows NT/2000) could not bind to its socket. A system call failed when the daemon (UNIX) or service (Windows NT/2000) attempted to bind to its configured port number. This is usually caused by another process having acquired the port before the daemon or service started.

Recommended Action:

1. Examine the NetBackup Problems and All Log Entries reports.

2. Create `bprd` and `bpdbm` activity log directories and retry the operation. Check the resulting logs to see the system error message resulting from the attempt.

   If another process has the port, use other system commands to determine the process. Based on this research, either change the port number in your `services` file or map or terminate the process that has acquired the port.

   On UNIX, another possible cause for this error is terminating `bprd` or `bpdbm` with the `kill` command. If you have to stop `bprd`, the recommended method is to use the Terminate Request Daemon option on the Special menu in `bpadm` (or the equivalent option in `xbpadm`). To stop `bpdbm`, use the `/usr/openv/netbackup/bin/bpdbm -terminate` command. Using the `kill` command to stop these processes can leave them unable to bind to their assigned ports the next time they are started.

   To identify a `bprd` or `bpdbm` problem, look for lines similar to the following in the activity log for the respective process:

```
<16> getsockbound: bind() failed, Address already in use (114)
<32> listen_loop: cannot get bound socket. errno = 114
<4> terminate: termination begun...error code = 146
```

   Similar entries can appear in the reports.

3. If the problem persists longer than ten minutes, it is possible that it will be necessary to reboot the server.

Status Code: 147

Message: required or specified copy was not found

Explanation: The requested copy number of a backup or archive image cannot be found.

Recommended Action: Correct the request to specify a copy number that does exist.

Status Code: 148

Message: daemon fork failed

Explanation: A NetBackup service could not create a child process due to an error received from the system. This is probably an intermittent error based on the availability of resources on the system.

Recommended Action:

1. Restart the service at a later time and investigate system problems that limit the number of processes.

2. Check the Event Viewer Application and System logs (Windows NT/2000).

Status Code: 150

Message: termination requested by administrator

Explanation: The process is terminating (or has terminated) as a direct result of a request from an authorized user or process.

Recommended Action: None.

Status Code: 151

Message: Backup Exec operation failed

Explanation: The Global Data Manager console has reported that a Backup Exec job (backup, archive, or restore) did not complete normally.

Recommended Action: Consult the Backup Exec job history on the Backup Exec server for details.

Status Code: 152

Message: required value not set

Explanation: An incomplete request was made to the `bpdbm` process (NetBackup Database Manager service on Windows NT/2000). This usually occurs because different versions of software are being used together.

Recommended Action:

1. Verify that all software is at the same version level.
2. For detailed troubleshooting information, create `bpdbm` and `admin` activity log directories and retry the operation. Check the resulting activity logs.

Status Code: 153

Message: server is not the master server

Explanation: This status code is reserved for future use.

Recommended Action: None.

Status Code: 154

Message: storage unit characteristics mismatched to request

Explanation: A backup was attempted and the storage unit selected for use had characteristics that were not compatible with the backup type.

Recommended Action: Verify that the characteristics of the storage unit involved are appropriate for the backup attempted:

- For an NDMP class type, verify that a storage unit of type NDMP is defined and the NDMP host value matches the host name of the client. For example, if the NDMP class specifies toaster as the client, the configuration for the storage unit must specify toaster as the NDMP host.
- For a class type other than NDMP, verify that the class specifies a Media Manager or Disk type storage unit.

Status Code: 158

Message: failed accessing daemon lock file

Explanation: The process could not lock its lock file because an error was received from a system call. This lock file synchronizes process activities (for example, preventing more than one daemon from executing at a time).

Recommended Action:

1. Examine the NetBackup error log to determine why the system call failed and correct the problem. It could be a permission problem.

2. If the error log does not show the error, create an activity log directory for `bprd`, `bpdbm`, or `bpsched` (depending on which process encountered the error) and retry the operation. Examine the resulting activity log.

Status Code: 159

Message: licensed use has been exceeded

Explanation: A configuration limit has been exceeded. An example is number of drives allowed per server.

Recommended Action: To determine the cause, examine the NetBackup error logs for the command that was being executed.

Status Code: 160

Message: authentication failed

Explanation: A problem was encountered when two systems were attempting to authenticate one another.

Recommended Action: See the *NetBackup System Administrator's Guide - UNIX* for more information on the files and commands mentioned here.

1. Ensure that the authentication libraries exist:

   Windows NT/2000, 98, 95:

   install_path`\NetBackup\lib\libvopie.dll`
   install_path`\NetBackup\lib\libnoauth.dll`

   UNIX (except HP-UX):

   ```
   /usr/openv/lib/libvopie.so
   /usr/openv/lib/libnoauth.so
   ```

   UNIX (HP-UX only):

   ```
   /usr/openv/lib/libvopie.sl
   /usr/openv/lib/libnoauth.sl
   ```

   Macintosh:

   ```
   :System Folder:Extensions:libvopie.dll
   :System Folder:Extensions:libnoauth.dll
   ```

2. Check the `methods_allow.txt` files on the systems that are having problems to ensure that authentication is enabled. The files are in the following locations:

Windows NT/2000, 98, 95:

install_path\NetBackup\var\auth

UNIX:

/usr/openv/var/auth

Macintosh:

:System Folder:Preferences:NetBackup:var:auth

3. On the systems that are having the authentication problem, remove the remote host that is not being authenticated from the methods_allow.txt file.

   For example, if hosta and hostb are having the problem, remove hosta from the file on hostb and vice versa.

   Retry the operation.

   - If the problem still exists, it indicates connection problems not related to authentication.
   - If connections are now successful, proceed to the next step.

4. Execute bpauthsync -vopie on the master server to resynchronize the key files on the systems.

   On Windows NT/2000:

   install_path\NetBackup\bin\admincmd\bpauthsync -vopie -servers -clients

   On UNIX:

   /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -servers -clients

5. Add back the names removed in step 3 and retry the operation.

6. Create activity log directories for the processes involved in authentication between NetBackup systems. These include:

   - On the server, create activity log directories for bprd, bpdbm, bpcd.
   - On the client, create activity log directories for bpbackup, bprestore, bpbkar (Windows NT/2000 only).

   Retry the operation and check the logs.

Status Code: 161

Message: Evaluation software has expired. See www.veritas.com for ordering information.

Explanation: The time allowed for the NetBackup evaluation software has ended.

Recommended Action: Obtain a licensed copy of NetBackup.

Status Code: 164

Message: unable to mount media because it is in a DOWN drive or misplaced

Explanation: A restore was attempted and the volume required for the restore was in a DOWN drive in a robot. Or, the slot that should contain the volume is empty.

Recommended Action:

- If volume is in a DOWN drive, remove it and place it in its designated slot. Then, retry the restore.
- If the volume is in the wrong slot, use a robot inventory option to reconcile the contents of the robot with the Media Manager volume configuration.

Status Code: 165

Message: NB image database contains no image fragments for requested backup id/copy number

Explanation: A restore was attempted and NetBackup has no record of fragments associated with the backup ID that has the files.

Recommended Action: Check the NetBackup Problems report for additional information about the error. For detailed troubleshooting information, create an activity log directory for either `bpdm` or `bptm` (whichever applies) and retry the operation. Check the resulting activity log.

Status Code: 166

Message: backups are not allowed to span media

Explanation: An end of media (EOM) was encountered while the backup image was being written. The backup was terminated because the NetBackup `DISALLOW_BACKUPS_SPANNING_MEDIA` option was present in `bp.conf` on UNIX or the registry on Windows NT/2000. The backup will be retried automatically with a different volume if this is allowed by the backup tries attribute in the NetBackup global attribute configuration.

Recommended Action: None.

Status Code: 167

Message: cannot find requested volume pool in Media Manager volume database

Explanation: A backup to a nonrobotic drive was attempted and the tape manager (`bptm`) could not find or add the specified volume pool.

Recommended Action: Verify the Media Manager volume configuration. Check the NetBackup Problems report for more information about the error. For detailed troubleshooting information, create a `bptm` activity log directory and retry the operation. Check the resulting activity log.

Status Code: 168

Message: cannot overwrite media, data on it is protected

Explanation: A catalog backup was attempted to a volume that could not be overwritten because it contains data that NetBackup, by default, does not overwrite (tar, cpio, ANSI, and so on).

Recommended Action: Replace the volume with a new one or set the NetBackup `ALLOW_MEDIA_OVERWRITE` option to the appropriate value.

Status Code: 169

Message: media id is either expired or will exceed maximum mounts

Explanation: A backup or catalog backup was attempted and the volume selected for use has reached its maximum number of mounts as specified in the Media Manager volume configuration. For a regular backup, the volume is automatically set to the SUSPENDED state and not used for further backups. For a NetBackup catalog backup, the operation terminates abnormally.

Recommended Action: If the volume was suspended, wait until it expires and then replace it. For NetBackup catalog backups, replace the media.

Status Code: 171

Message: media id must be 6 or less characters

Explanation: An operation, such as using `bpmedia` to suspend or freeze a media ID, was attempted and the media ID specified was longer than six alpha-numeric characters.

Recommended Action: Retry the command with a valid media ID.

Status Code: 172

Message: cannot read media header, may not be NetBackup media or is corrupted

Explanation: When loading a volume for a backup or restore, the tape manager (bptm), did not find the expected tape header. This can mean that a volume in a robotic device is not in the slot number shown in the Media Manager volume configuration or that a read error (I/O error) occurred.

Recommended Action:

1. If the volume is in a robot that supports barcodes, verify the robot contents by using a Media Manager robot inventory option.

2. If the volume was mounted on a nonrobotic drive, verify that the correct volume was mounted and assigned.

3. Check the NetBackup Problems report. If a fatal read error occurred, attempt the operation again using another drive, if possible.

Status Code: 173

Message: cannot read backup header, media may be corrupted

Explanation: When searching for a backup image to restore, the tape manager (bptm) could not find the correct backup ID at the position on the media where NetBackup expected it to be. This can indicate a drive hardware problem.

Recommended Action:

1. Check the NetBackup Problems report for clues as to what caused the error.

2. Try the restore on another drive if possible.

3. For detailed troubleshooting information, create an activity log directory for bptm and retry the operation. Check the resulting activity log.

Status Code: 174

Message: media manager system error occurred

Explanation: An abnormal condition occurred causing a tape manager (bptm) or disk manager (bpdm) failure. This should not occur under normal circumstances.

Note If this occurs on a Sequent platform and you are attempting to back up more than four gigabytes of data, save all your logs and call VERITAS technical support. For other platforms perform the recommended actions described below.

Recommended Action:

1. Check the NetBackup Problems report to see if it shows the cause of the problem. If you see a Problems report message similar to

```
"attempting to write 32767 bytes, not a multiple of 1024"
```

   save all logs and call VERITAS customer support.

2. On UNIX, if this occurs during a restore, it may be that the tape drive is incorrectly configured to write in fixed length mode when it should write in variable length mode.

   Verify your drive's configuration, comparing it to what is recommended in the *Media Manager Device Configuration Guide* (also see step 7 of this procedure).

   If your configuration incorrectly specifies fixed length mode, change the configuration to specify variable length mode and suspend media that were written on that device. The images written to those media may be restorable (this is platform dependent), but single file restores are almost guaranteed to fail.

3. If you see the problem with only one client, verify that the client binaries are correct, especially those for `bpcd`.

4. Can you read or write any other images on this media?

   If so, check the following reports for clues:

   - Images on Media report
   - Media Contents report

5. Verify the following:

   - The media by using the NetBackup image verify option.
   - That you are using the correct media type for the device.

6. Check the system or console log for errors (on UNIX) or the Event Viewer Application log (on Windows NT/2000).

7. For detailed debug information, create an activity log directory for either `bptm` or `bpdm` (whichever applies) and retry the operation. Check the resulting activity log.

   If the `bptm` activity log shows an error similar to

```
00:58:54 [2304] <16> write_data: write of 32768 bytes
indicated only 29696 bytes were written, errno = 0
```

   it may be that the tape drive is configured to write in fixed length mode rather than variable length mode, and the image being written encountered the end-of-media.

   Take the corrective action suggested in step 2.

Status Code: 175

Message: not all requested files were restored

Explanation: When restoring files from an image, the `bptm` or `bpdm` process detected a fatal error condition and terminated the restore before it completed. This should not occur under normal circumstances.

Recommended Action:

1. Check the NetBackup Problems report and the progress log on the client for additional information about the error

2. For detailed troubleshooting information, create an activity log directory for either `bptm` or `bpdm` (whichever applies) and retry the operation. Check the resulting activity log.

Status Code: 176

Message: cannot perform specified media import operation

Explanation: The tape manager (`bptm`) detected an error condition when attempting to import a specific backup image. Possible reasons for this are:

- Media ID is already active in the NetBackup media catalog on this server
- Media ID is not in the Media Manager volume configuration
- Fatal tape manager (`bptm`) error occurred
- Total image was not obtained from Phase 1 of import

Recommended Action:

1. Check the NetBackup Problems report to find the exact cause of the failure.

2. Try the following:
   - If the media ID is already active, duplicate all images on the original media ID to another volume. Then, manually expire the original media and redo the import.
   - If the media ID is not present in the Media Manager volume configuration, add it.
   - If a fatal `bptm` error occurred, verify that the Media Manager volume daemon (`vmd`) is active on UNIX or the NetBackup Volume Manager service is active on Windows NT/2000.
   - If the entire image is not present, perform import phase 1 on the media IDs that have the remainder of the image.

Status Code: 177

Message: could not deassign media due to Media Manager error

Explanation: The tape manager (`bptm`) could not successfully deassign a media ID.

Recommended Action:

1. Check the NetBackup Problems report for the cause of the problem.
2. Verify that the Media Manager volume daemon (`vmd`) is active on UNIX or the NetBackup Volume Manager service is active on Windows NT/2000.
3. For detailed troubleshooting information, create an activity log directory for `bptm` and retry the operation. Check the resulting activity log.

Status Code: 178

Message: media id is not in NetBackup volume pool

Explanation: NetBackup attempted a backup of its catalogs and the media ID specified for the catalog backup was not in the NetBackup volume pool. Volumes for catalog backups must be in the NetBackup volume pool.

Recommended Action: Check the Media Manager volume configuration to verify that the media IDs are present and in the NetBackup volume pool.

Status Code: 179

Message: density is incorrect for the media id

Explanation: An operation such as "list contents" was attempted on an invalid media ID, such as a cleaning tape. Another possibility is that a media ID in the NetBackup catalog backup configuration does not match the media type entered in the Media Manager volume configuration.

Recommended Action: Check the volume configuration and the NetBackup catalog backup configuration and correct any problems found.

Status Code: 180

Message: tar was successful

Explanation: `tar` returned a successful exit status.

Recommended Action: None.

Status Code: 181

Message: tar received an invalid argument

Explanation: One of the parameters passed to `tar` was not valid.

Recommended Action: On a UNIX client:

- Ensure that the `tar` command in `/usr/openv/netbackup/bin` is the one provided by NetBackup. If you are in doubt, reinstall it.
- Check `/usr/openv/netbackup/bin/version` on the client to verify that the client is running the correct level software. If the software is not at the correct level, update the software per the directions in the NetBackup release notes.

On a Windows NT/2000 client, create a `tar` activity log directory, retry the operation, and check the log.

On a Macintosh client, check the version file that is in the bin folder in the NetBackup folder in the Preferences folder. If the software is not at the correct level, install the correct software as explained in the installation guide.

Status Code: 182

Message: tar received an invalid file name

Explanation: `tar` cannot write to the file that is specified with the `-f` parameter.

Recommended Action:

1. Create a `bpcd` activity log directory on the client (on a Macintosh NetBackup creates the log automatically).
2. On a Windows NT/2000 client, create a `tar` activity log directory.
3. Increase the logging level on the client:
   - On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
   - On PC clients, increase the debug or log level as explained in the activity log topics in Chapter 3.
4. Rerun the operation, check the resulting activity logs for the parameters passed to `tar` and call customer support.

Status Code: 183

Message: tar received an invalid archive

Explanation: The data passed to `tar` was corrupt.

Recommended Action:

- If the problem is with a UNIX client, create a `/usr/openv/netbackup/logs/tar` activity log directory on the client and rerun the operation.

  a. Check the `tar` activity log file for error messages that explain the problem.

  b. Reboot the client to see if this clears the problem.

  c. When you are through investigating the problem, delete the `/usr/openv/netbackup/logs/tar` directory on the client.

- If the problem is with a Microsoft Windows, NetWare, or Macintosh client:

  a. Create a `bpcd` activity log directory on the client (on a Macintosh NetBackup creates the log automatically).

  b. On a Windows NT/2000 client, create a `tar` activity log directory.

  c. Increase the debug or log level as explained in the activity log topics in Chapter 3.

  d. Rerun the operation and check the resulting activity logs.

  e. Reboot the client to see if it clears the problem.

Status Code: 184

Message: tar had an unexpected error

Explanation: A system error occurred in `tar`.

Recommended Action:

- If the problem is with a UNIX client, create a `/usr/openv/netbackup/logs/tar` activity log directory on the client and rerun the operation.Create a `/usr/openv/netbackup/logs/tar` directory on the client and rerun the operation.

  a. Check the `tar` activity log file for error messages that explain the problem.

  b. Reboot the client to see if this clears the problem.

  c. When you are through investigating the problem, delete the `/usr/openv/netbackup/logs/tar` directory on the client.

- If the problem is with a Microsoft Windows, NetWare, or Macintosh client:

a. Create a `bpcd` activity log directory on the client (on a Macintosh NetBackup creates the log automatically).

b. Increase the debug or log level as explained in the activity log topics in Chapter 3.

c. On a Windows NT/2000 client, create a `tar` activity log directory.

d. Retry the operation and check the resulting activity logs.

e. Reboot the client to see if it clears the problem.

Status Code: 185

Message: tar did not find all the files to be restored

Explanation: There were files in the `tar` file list that were not in the image.

Recommended Action:

- If the problem is with a UNIX client:

  a. Enable `bpcd` activity logging by creating the `/usr/openv/netbackup/logs/bpcd` directory on the client.

  b. Rerun the operation, check the resulting `bpcd` log file for the parameters passed to `tar`, and call customer support.

- If the problem is with a Microsoft Windows, NetWare, or Macintosh client:

  a. Create a `bpcd` activity log directory on the client (on a Macintosh NetBackup creates the log automatically).

  b. Increase the debug or log level as explained in the activity log topics in Chapter 3.

  c. On a Windows NT/2000 client, create a `tar` activity log directory.

  d. Retry the operation.

  e. Check the resulting activity logs for the parameters passed to `tar` and call customer support.

Status Code: 186

Message: tar received no data

Explanation: The media manager did not send data to `tar`.

Recommended Action:

1. Retry the operation and check the progress log on the client for error messages that reveal the problem.
2. Verify that the tape is available and readable.
3. Verify that the drive is in an UP state. Use the Device Monitor
4. For detailed troubleshooting information:
   a. Create a `bptm` activity log on the server.
   b. On a Windows NT/2000 client, create a `tar` activity log.
   c. Retry the operation and check the resulting activity logs.

Status Code: 189

Message: the server is not allowed to write to the client's filesystems

Explanation: The client is not allowing writes from the server.

Recommended Action: Perform the following to perform restores or install software from the server.

- On a UNIX client, delete `DISALLOW_SERVER_FILE_WRITES` from the `/usr/openv/netbackup/bp.conf` file.
- On a Microsoft Windows or NetWare nontarget client, select Allow server-directed restores on the General tab in the NetBackup Configuration dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and click Configure on the Actions menu.
- On a Macintosh client, delete `DISALLOW_SERVER_FILE_WRITES` from the `bp.conf` file in the NetBackup folder in the Preferences folder.
- On a NetWare target client, set `ALLOW_SERVER_WRITE` to yes in the `bp.ini` file.

Status Code: 190

Message: found no images or media matching the selection criteria

Explanation: A verify, duplicate, or import was attempted and no images matching the search criteria were found in the NetBackup catalog.

Recommended Action: Change the search criteria and retry.

Status Code: 191

Message: no images were successfully processed

Explanation: A verify, duplicate, or import was attempted and failed for all selected images.

Recommended Action: Check the NetBackup Problems report for the cause of the error. To obtain detailed troubleshooting information, create an `admin` activity log directory and retry the operation. Check the resulting activity log.

Status Code: 194

Message: the maximum number of jobs per client is set to 0

Explanation: The NetBackup Maximum jobs per client global attribute is currently set to 0. Setting the value to 0 disables backups and archives.

Recommended Action: To enable backups and archives, change the Maximum jobs per client value to the desired nonzero setting. This attribute is on the Global NetBackup Attributes tab in the Master Server Properties dialog box. See "Using the Configure - NetBackup Window" on page 57.

Status Code: 195

Message: client backup was not attempted

Explanation: A backup job was in the NetBackup scheduler's worklist but was not attempted.

Recommended Action:

1. Retry the backup either immediately with a manual backup or allow the normal scheduler retries.

2. For additional information, check the All Log Entries report. For detailed troubleshooting information, create a `bpsched` activity log directory on the master server. After the next backup attempt, check the activity log.

   Some actions to perform are:

   - Verify that the `vmd` and `ltid` daemons (UNIX) or the NetBackup Volume Manager and NetBackup Device Manager services (Windows NT/2000) are running.
   - Look for a problem in an earlier backup that made the media or storage unit unavailable.

Status Code: 196

Message: client backup was not attempted because backup window closed

Explanation: A backup or archive operation that was queued by the backup scheduler was not attempted because the backup window was no longer open.

Recommended Action:

- If possible, change the schedule to extend the backup window for this class and schedule combination so it does not occur again.
- If the backup must be run, use the Manual Backup command on the Class menu in the Backup Policy Management window to perform the backup. Manual backups ignore the backup window.

Status Code: 197

Message: the specified schedule does not exist in the specified class

Explanation: A user backup or archive request has specified the exact class and schedule to use when performing a backup. The class exists but does not contain the schedule.

- On Microsoft Windows and NetWare nontarget clients, you can specify a class or schedule on the Backups tab in the NetBackup Configuration dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and click Configure on the Actions menu.
- On UNIX and Macintosh clients, you can specify a class or schedule by using the `bp.conf` options, `BPBACKUP_CLASS` or `BPBACKUP_SCHED`.
- On NetWare target clients, you can specify a class or schedule in the `bp.ini` file.

Recommended Action:

1. Check the client progress log (if available) to determine the class and schedule that were specified.
2. Check the configuration on the master server to determine if the schedule is valid for the class. If the schedule is not valid, either add the schedule to the class configuration or specify a valid schedule on the client.

Status Code: 198

Message: no active classes contain schedules of the requested type for this client

Explanation: A user backup or archive has been requested, and this client is not in a class that has a user backup or archive schedule.

Recommended Action: Determine if the client is in any class that has a schedule of the appropriate type (either user backup or archive).

- If the client is in such a class, check the general class attributes to verify that the class is set to active.

- If the client is not in such a class, either add a schedule of the appropriate type to an existing class that has this client or create a new class that has this client and a schedule of the appropriate type.

Status Code: 199

Message: operation not allowed during this time period

Explanation: A user backup or archive has been requested and this client is not in a class that has a user backup or archive schedule with an open backup window. This error implies that there is an appropriate class and schedule combination for this client.

Recommended Action: Determine the classes to which this client belongs that also have a schedule of the appropriate type (either user backup or archive).

- If possible, retry the operation when the backup window is open.
- If the backup window is not open during appropriate time periods, adjust a backup window for a schedule in one of the classes.

Status Code: 200

Message: scheduler found no backups due to run

Explanation: When checking the class and schedule configuration, the NetBackup scheduler process (`bpsched`) did not find any clients to back up. This could be due to:

- No backup time windows are open (applies only to full and incremental schedules).
- Classes are set to inactive.
- The clients were recently backed up and are not due for another backup (based on Frequency setting for the schedules).
- Classes do not have any clients.

Recommended Action: Usually, this message can be considered informational and does not indicate a problem. However, if you suspect a problem:

1. Examine the NetBackup All Log Entries report to see if there are any messages in addition to one indicating that the scheduler found nothing to do.
2. Examine the class configuration for all classes or the specific class in question and determine if any of the reasons mentioned in the Explanation section above apply.
3. To obtain detailed troubleshooting information, create a `bpsched` activity log directory on the master server and retry the operation. Check the resulting activity log.

Status Code: 201

Message: handshaking failed with server backup restore manager

Explanation: A process on the master server encountered an error when communicating with the media host (can be either the master or a media server). This error means that the master and media server processes were able to initiate communication, but encountered difficulties in completing them. This problem can occur during a backup, restore, or media list in a single or multiple server configuration.

Recommended Action:

1. Determine the activity that encountered the handshake failure by examining the NetBackup All Log Entries report for the appropriate time period. If there are media servers, determine if:
   - The handshake failure was encountered between the master and a media server.

     or
   - Only the master server was involved.
2. If necessary, create the following activity log directories for the following:
   - `bpcd` on the NetBackup media host (can be either the master or a media server).
   - If the error was encountered during a backup operation, `bpsched` on the master server.
   - If the error was encountered during a restore operation, `bprd` on the master server.
   - If the error was encountered during a media list operation, `admin` in the NetBackup `logs/admin` directory on the master server.
3. Retry the operation and examine the resulting activity logs for information on why the error occurred.

Status Code: 202

Message: timed out connecting to server backup restore manager

Explanation: A process on the master server timed out while trying to initiate communications with the media host (can be either the master or a media server). This problem can occur during a backup or restore in either a single or multiple server configuration.

Recommended Action: Determine which activity encountered the connection timeout failure by examining the All Log Entries report for the appropriate time period. If there are media servers, determine if the timeout occurred between the master and a media server or if only the master was involved.

1. Verify that the schedule specifies the correct storage unit.

2. Execute the `ping` command from one host to another by using the following combinations:

   - From the master server, ping the master and all media servers by using the host names found in the storage unit configuration.
   - From each of the media servers, ping the master server by using the host name specified in the NetBackup server list. On a UNIX server, this is the first `SERVER` entry in the `bp.conf` file. On a Windows NT/2000 server, the master is designated on the Servers tab in the Master Server Properties dialog. To access this dialog, see "Using the Configure - NetBackup Window" on page 57.

3. Verify that the master server can communicate with `bpcd` on the host that has the storage unit.

   After each backup, the scheduler checks the storage unit to see how many drives are available (in case the backup caused a drive to be automatically downed). If `bpsched` cannot communicate with `bpcd`, it sets the number of available drives in that storage unit to 0 and further backups to that storage unit fail.

   The available drives remain at 0 until the scheduler is initialized again. Therefore, even if `bpcd` seems to be operating correctly now, check the `bpsched` and `bpcd` activity logs (see below) for records of an earlier failure.

4. See "Testing Media Server and Clients" on page 21 and "Resolving Network Communication Problems" on page 24.

5. If necessary, create activity log directories for the following processes and retry the operation. Then, check the resulting activity logs on the master server:

   - If the error occurred during a backup operation, check the `bpsched` activity logs. Also, check the `bpcd` activity logs.
   - If the error occurred during a restore operation, check the `bprd` activity logs.

Status Code: 203

Message: server backup restore manager's network is unreachable

Explanation: A process on the master server could not connect to a particular host on the network when trying to initiate communication with the media host for a particular operation. This problem can occur during a backup or restore in either a single or multiple server configuration.

Recommended Action: Determine which activity encountered the network unreachable failure by examining the All Log Entries report for the appropriate time frame. If there is more than one NetBackup server (that is, one or more media servers) determine if the

network unreachable failure was encountered between the master and a media server or if only the master server was involved. Execute the `ping` command from one host to another by using the following combinations:

1. From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

2. From each of the media servers, ping the master server host by using the host name specified in the NetBackup server list. On a UNIX server, this is the first `SERVER` entry in the `bp.conf` file. On a Windows NT/2000 server, the master is designated on the Servers tab in the Master Server Properties dialog. To access this dialog, see "Using the Configure - NetBackup Window" on page 57.

3. See "Testing Media Server and Clients" on page 21 and "Resolving Network Communication Problems" on page 24.

4. If necessary, create activity log directories for the following processes and retry the operation. Then, check the resulting activity logs on the master server:
   - If the error occurred during a backup, check the `bpsched` activity logs.
   - If the error occurred during a restore, check the `bprd` activity logs.

Status Code: 204

Message: connection refused by server backup restore manager

Explanation: The media host refused a connection on the port number for `bpcd`. This error can be encountered during a backup or restore.

Recommended Action: Execute the `ping` command from one host to another by using the following combinations:

Note Also, see "Resolving Network Communication Problems" on page 24.

1. From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

2. From each of the media servers, ping the master server by using the name specified in the NetBackup server list. On a UNIX server, this is the first `SERVER` entry in the `bp.conf` file. On a Windows NT/2000 server, the master is designated on the Servers tab in the Master Server Properties dialog. To access this dialog, see "Using the Configure - NetBackup Window" on page 57.

3. On UNIX servers, verify that the bpcd entries in /etc/services or NIS on all the servers are identical. Verify that the media host is listening on the correct port for connections to bpcd by running one of the following commands (depending on platform and operating system):

   ```
   netstat -a | grep bpcd
   ```

   ```
   netstat -a | grep 13782
   ```
   (or the value specified during the install)

   ```
   rpcinfo -p | grep 13782
   ```
   (or the value specified during the install)

   On UNIX servers, you may have to change the service number for bpcd in /etc/services and the NIS services map and send SIGHUP signals to the inetd processes on the clients.

   ```
   /bin/ps -ef | grep inetd
   kill -HUP the_inetd_pid
   ```

   or

   ```
   /bin/ps -aux | grep inetd
   kill -HUP the_inetd_pid
   ```

Note On a Hewlett-Packard UNIX platform, use `inetd -c` to send a SIGHUP to inetd.

4. On Windows NT/2000 servers:

   a. Verify that the bpcd entries are correct in:

      ```
      %SystemRoot%\system32\drivers\etc\services
      ```

   b. Verify that the NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog match the settings in the services file. To display this dialog, start the Backup, Archive, and Restore interface and click Configure on the Actions menu.

      The values on the Network tab are written to the services file when the NetBackup Client service starts.

   c. Stop and restart the NetBackup services.

5. See "Testing Media Server and Clients" on page 21 and "Resolving Network Communication Problems" on page 24.

6. If necessary, create activity log directories for the following processes and retry the operation. Then, check the resulting activity logs on the master server:

   - If the error occurred during a backup operation, check the bpsched activity logs.

- If the error occurred during a restore operation, check the bprd activity logs.

Status Code: 205

Message: cannot connect to server backup restore manager

Explanation: A process on the master server could not connect to a process on a host on the network while trying to initiate communication with the server that has the storage unit for a particular operation. This problem can occur during a backup or restore in either a single or multiple server configuration. This can also occur when the scheduler process (bpsched) is building its list of available storage units to use during backups.

Recommended Action: Execute the ping command from one host to another by using the following combinations:

Note Also, see "Resolving Network Communication Problems" on page 24.

1. From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

2. From each of the media servers, ping the master server by using the name specified in the NetBackup server list. On a UNIX server, this is the first SERVER entry in the bp.conf file. On a Windows NT/2000 server, the master is designated on the Servers tab in the Master Server Properties dialog. To access this dialog, see "Using the Configure - NetBackup Window" on page 57.

3. On a UNIX server, verify that the bpcd entry in /etc/services or NIS on all the servers are identical. Verify that the media host is listening on the correct port for connections to bpcd by running one of the following commands (depending on platform and operating system):

   ```
   netstat -a | grep bpcd
   ```

   ```
   netstat -a | grep 13782
   ```
   (or the value specified during the install)

   ```
   rpcinfo -p | grep 13782
   ```
   (or the value specified during the install)

4. On Windows NT/2000 servers:

   a. Verify that the bpcd entries are correct in the services file:

      ```
      %SystemRoot%\system32\drivers\etc\services
      ```

   b. Verify that the NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Configuration dialog match the settings in the services file. To display this dialog, start the Backup, Archive, and Restore interface and click Configure on the Actions menu.

The values on the Network tab are written to the `services` file when the NetBackup Client service starts.

c. Stop and restart the NetBackup services.

5. See "Testing Media Server and Clients" on page 21 and "Resolving Network Communication Problems" on page 24.

6. Create a `bpcd` activity log directory on the server that has the storage unit and retry the operation. Then, check for additional information in the resulting activity log.

Status Code: 206

Message: access to server backup restore manager denied

Explanation: The master server is trying to start a process on another server (or itself) and the master server does not appear in the Netbackup server list on that server. On a UNIX server, the master is the first `SERVER` entry in the `bp.conf` file. On a Windows NT/2000 server, the master is designated on the Servers tab in the Master Server Properties dialog. To access this dialog, see "Using the Configure - NetBackup Window" on page 57.

Recommended Action:

1. Verify that the master server appears as a server in its own server list as well as being listed on all media servers.

   If you change the server list on a master server, stop and restart the NetBackup database manager and request daemons (UNIX) or the NetBackup Database Manager and NetBackup Request Manager services (Windows NT/2000).

2. If necessary, create activity log directories for the following processes and retry the operation. Then, check the resulting activity logs on the master server:
   - If the error occurred during a backup operation, check the `bpsched` activity logs.
   - If the error occurred during a restore operation, check the `bprd` activity logs.

Status Code: 207

Message: error obtaining date of last backup for client

Explanation: An error occurred when the backup scheduler (`bpsched`) tried to obtain the date of the last backup for a particular client, class, and schedule combination.

Recommended Action:

1. Verify that the NetBackup database manager (bpdbm) process (NetBackup Database Manager service on Windows NT/2000) is running.

2. Examine the All Log Entries report for the appropriate time frame to gather more information about the failure.

3. For detailed troubleshooting information, create activity log directories for bpsched and bpdbm on the master server and retry the operation. Then, check the resulting activity logs.

Status Code: 208

Message: failed reading user directed file list

Explanation: An error occurred when the backup scheduler (bpsched) attempted to read the list of files requested for a user backup or archive. This error indicates either a client-server communication problem, or a system problem on the master server where the NetBackup scheduler process (bpsched) is running.

Recommended Action: For detailed troubleshooting information, create activity log directories for bpsched and bprd on the master server and retry the operation. Then, check the resulting activity logs.

Status Code: 209

Message: error creating or getting message queue

Explanation: An error occurred when the backup scheduler (bpsched) attempted to create an internal message queue construct for interprocess communication. This error indicates a problem on the master server and is most likely due to a lack of system resources for System V interprocess communication.

Recommended Action: Create a bpsched activity log directory on the master server and retry the operation. Then, determine the type of system failure by examining the error message in the bpsched activity log.

On UNIX servers, also gather the output of the ipcs -a command to see what system resources are currently in use.

Status Code: 210

Message: error receiving information on message queue

Explanation: An error occurred when one of the backup scheduler (bpsched) processes attempted to receive a message from another bpsched process on an internal message queue construct. This error indicates a problem on the master server and is likely due to problems with or a lack of system resources for System V interprocess communication.

Recommended Action: Create a `bpsched` activity log directory on the master server and retry the operation. Then, determine the type of system failure by examining the error message in the `bpsched` activity log on the master server.

On UNIX servers, also gather the output of the `ipcs -a` command to see what system resources are currently in use.

Status Code: 211

Message: scheduler child killed by signal

Explanation: A backup scheduler (`bpsched`) child process, which interacts with the backup restore manager (`bpbrm`) on the media host, was terminated. This can occur because of system administrator action.

Recommended Action: Create an activity log directory for `bpsched` on the master server and retry the operation. Then, to determine the cause of the child termination, examine the messages in the `bpsched` activity log.

Status Code: 212

Message: error sending information on message queue

Explanation: The backup scheduler (`bpsched`) encountered an error when attempting to attach to an already existing internal message queue construct for interprocess communication. This error indicates a problem on the master server and is likely due to a lack of system resources for System V interprocess communication.

Recommended Action: Create a `bpsched` activity log directory on the master server and retry the operation. Then, determine the type of system failure by examining the error message in the `bpsched` activity log.

On a UNIX server, also, gather the output of the `ipcs -a` command to see what system resources are currently in use.

Status Code: 213

Message: no storage units available for use

Explanation: The NetBackup scheduler process (`bpsched`) did not find any of its storage units available for use. Either all storage units are unavailable or all storage units are configured for On demand only and the class and schedule does not require a specific storage unit.

Recommended Action:

1. Examine the Backup Status and All Log Entries report for the appropriate time period to determine the class or schedule that received the error.

2. Verify that the storage unit's drives are not down or waiting for media from a previous operation that did not complete.

3. Verify that all the storage units do not have their Maximum concurrent jobs attribute set to 0 (for disk storage units) and Maximum concurrent drives used for backup attribute set to 0 (for Media Manager storage units).

4. Verify that the robot number and host name in the storage unit configuration matches the Media Manager device configuration.

5. Determine if all storage units are set to On demand only for a class and schedule combination that does not require a specific storage unit. If this is the case, either specify a storage unit for the class and schedule combination or turn off On demand only for a storage unit.

6. If the storage unit is on a UNIX NetBackup media server, it could indicate a problem with `bpcd`. Check `/etc/inetd.conf` on the media server to verify that the `bpcd` entry is ok.

   If the storage unit is on a Windows NT/2000 NetBackup media server, verify that the NetBackup Client service has been started on the Windows NT/2000 NetBackup media server.

7. For detailed troubleshooting information, create a `bpsched` activity log directory on the master server and retry the operation. Then, check the resulting activity log.

Status Code: 214

Message: regular bpsched is already running

Explanation: The NetBackup scheduler (`bpsched`) performs periodic checking of the class and schedule configuration to determine if there are new backups due. Error 214 indicates that when a new instance of NetBackup starts, it finds that a scheduler process is already checking the class and schedule configuration.

Recommended Action: Usually, no action is required for this condition. However, *NEVER* kill `bpsched` before doing some checking. For example, `bpsched` could be calling `bpdbm` (NetBackup Database Manager service on Windows NT/2000) to clean up and compress the catalogs.

To determine what the running `bpsched` is currently doing, examine the `bpsched` activity log on the master server. If necessary, enable `bpsched` activity logging by creating a `bpsched` activity log directory on the master server and retrying the operation.

To check for backups do the following:

On a UNIX master server:

1. Check for active or queued backups by using the job monitor.

2. Check for active `bp` processes with `bpps`. This reveals if there are `bpbrm` or `bptm` processes running and a backup is active.

3. If there is no reason for `bpsched` to be running, then use `kill -HUP` to terminate it.

Status Code: 215

Message: failed reading global config database information

Explanation: During the periodic checking of the NetBackup configuration, the NetBackup scheduler process (`bpsched`) was unable to read the global configuration parameters.

Recommended Action:

1. On a UNIX master server, verify that the NetBackup database manager (`bpdbm`) process is running. On a Windows NT/2000 master server, verify that the NetBackup Database Manager service is running.

2. Attempt to view the global configuration settings by using the NetBackup administration interface.

3. For detailed troubleshooting information, create activity log directories for `bpsched` and `bpdbm` on the master server and retry the operation. Then, check the resulting activity logs.

Status Code: 216

Message: failed reading retention database information

Explanation: During its periodic checking of the NetBackup configuration, the NetBackup scheduler process (`bpsched`) could not read the list of retention levels and values.

Recommended Action:

1. On a UNIX master server, verify that the NetBackup database manager (bpdbm) process is running. On a Windows NT/2000 master server, verify that the NetBackup Database Manager service is running.

2. For detailed troubleshooting information, create activity log directories for bpsched and bpdbm on the master server and retry the operation. Then, check the resulting activity logs.

Status Code: 217

Message: failed reading storage unit database information

Explanation: During its periodic checking of the NetBackup configuration, the NetBackup scheduler process (bpsched) could not read the storage unit configuration.

Recommended Action:

1. On a UNIX server, verify that the NetBackup database manager (bpdbm) process is running. On a Windows NT/2000 server, verify that the NetBackup Database Manager service is running.

2. Attempt to view the storage unit configuration by using the NetBackup administration interface.

3. For detailed troubleshooting information, create activity logs for bpsched and bpdbm on the master server and retry the operation. Then, check the resulting activity logs.

   Ensure that the correct master server is being specified for the connection.

Status Code: 218

Message: failed reading class database information

Explanation: During the periodic checking of the NetBackup configuration, the NetBackup scheduler process (bpsched) could not read the class (backup policy) configuration.

Recommended Action:

1. On a UNIX server, verify that the NetBackup Database Manager (bpdbm) process is running. On a Windows NT/2000 server, verify that the NetBackup Database Manager service is running.

2. Attempt to view the class configuration by using the NetBackup administration interface.

3. For detailed troubleshooting information, create activity log directories for `bpsched` and `bpdbm` on the master server and retry the operation. Then, check the resulting activity logs.

   Ensure that the correct master server is being specified for the connection.

Status Code: 219

Message: the required storage unit is unavailable

Explanation: The class or schedule for the backup requires a specific storage unit, which is currently unavailable. This error also occurs for other attempts to use the storage unit within the current backup session.

Recommended Action: Look in the Job Details window for the failed job. Or, examine the Backup Status and All Log Entries report for the appropriate time period to determine the class or schedule that received the error; then examine the specific class and schedule configuration to determine the required storage unit.

1. Verify that the schedule specifies the correct storage unit and the storage unit exists.

2. Verify that the Media Manager device daemon (`ltid`) is running (if the server is UNIX) or the NetBackup Device Manager service is running (if the server is a Windows NT/2000 system). Use `bpps` on UNIX and the Activity Monitor on Windows NT/2000.

3. Verify that the storage unit does not have the Maximum concurrent jobs attribute set to 0 (for a disk storage unit) and the Maximum concurrent drives used for backup attribute set to 0 (for a Media Manager storage unit).

4. If the storage unit is a tape or optical disk, verify that at least one of the drives is in the UP state. Use the Device Monitor (on UNIX `xdevadm` can also be used).

5. Verify that the robot number and host in the storage unit configuration matches what is specified in the Media Manager device configuration.

6. Verify that the master server can communicate with the `bpcd` process on the server that has the storage unit.

   a. Verify that `bpcd` is listening on the port for connections.

      On a UNIX server, executing

      ```
      netstat -a | grep bpcd
      ```

      should return something similar to the following:

      ```
      *.bpcd    *.*         0      0      0      0 LISTEN
      ```

Do this on the server where the storage unit is connected.

On a Windows NT/2000 NetBackup server, executing

```
netstat -a
```

prints out several lines of output. If bpcd is listening, one of those lines is similar to the following:

```
TCP    myhost:bpcd            0.0.0.0:0              LISTENING
```

Do this on the server where the storage unit is connected.

b. If bpcd seems to be operating correctly, create bpsched and bpcd activity log directories and retry the operation. Check the resulting activity logs for records of an earlier failure.

After each backup, the scheduler checks the storage unit to see how many drives are available (in case the backup caused a drive to be automatically downed). If bpsched cannot communicate with bpcd, it sets the number of available drives in that storage unit to 0 and further backups to that storage unit during this backup session will fail.

The number of available drives remains at 0 until the scheduler is initialized again.

c. If the cause of the problem is not obvious, perform some of the steps in "Resolving Network Communication Problems" on page 24.

Status Code: 220

Message: database system error

Explanation: The bpdbm process (NetBackup Database Manager service on Windows NT/2000) could not create a directory path for its configuration catalogs due to the failure of a system call. This is usually due to a permission problem or an "out of space" condition.

Recommended Action: Create an activity log directory for bpdbm and retry the operation. Check the resulting activity log for information.

Status Code: 221

Message: continue

Explanation: This status code is used in coordinating communication between various NetBackup processes and normally does not occur. If the logs show that it is associated with a subsequent error, it usually indicates a communication problem. In this case, concentrate your troubleshooting efforts on the subsequent error.

Recommended Action: Determine the cause of the status code that follows this one.

Status Code: 222

Message: done

Explanation: This status code is used in coordinating communication between various NetBackup processes and is normally not seen. If the error logs show that it is associated with a subsequent error, it usually indicates a communication problem. In this case, concentrate your troubleshooting efforts on the subsequent error.

Recommended Action: Determine the cause of the status code that follows this one.

Status Code: 223

Message: an invalid entry was encountered

Explanation: A request to the `bpdbm` process (NetBackup Database Manager service on Windows NT/2000) had invalid or conflicting information. This is usually a result of using software from different versions together, but can also be caused by incorrect parameters on a command.

Recommended Action: Verify that all NetBackup software is at the same version level and the command parameters are specified correctly. If neither of these is the problem, obtain detailed troubleshooting information by creating a `bpdbm` activity log directory and retrying the operation. Check the resulting activity log.

Status Code: 224

Message: there was a conflicting specification

Explanation: A request to the `bpdbm` process (NetBackup Database Manager service on Windows NT/2000) had conflicting information. This is usually a result of using software from different version levels together.

Recommended Action: Verify that all NetBackup software is at the same version level. If that is not the problem, obtain detailed troubleshooting information by creating `bpdbm` and `admin` activity log directories and retrying the operation. Check the resulting activity logs.

Status Code: 225

Message: text exceeded allowed length

Explanation: A request containing text that exceeds a buffer size was made to the `bpdbm` process (NetBackup Database Manager service on Windows NT/2000). This is usually a result of using software from different version levels together.

Recommended Action: Verify that all NetBackup software is at the same version level. If that is not the problem, create activity log directories for `bpdbm` and `admin`. Then, retry the operation and examine the resulting activity logs.

Status Code: 226

Message: the entity already exists

Explanation: The configuration already has an entity with the same name or definition. For example, you see this status if you try to add a new class when an existing class has the same name or definition (attributes, clients, and so on).

Recommended Action: Correct your request and re-execute the command.

Status Code: 227

Message: no entity was found

Explanation: The item requested was not in the catalog. For example, the entity could be a file or class information.

Recommended Action: A common cause for this problem is a query that has no matching images. Specify different parameters or options for the operation and try it again.

Status Code: 228

Message: unable to process request

Explanation: An inconsistency exists in the catalog or a request was made that would be improper to satisfy.

Recommended Action:

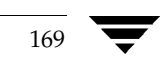
1. If this involves a media server, verify that its server list specifies the correct master server. On a UNIX server, the master server is the first `SERVER` entry in the `bp.conf` file. On a Windows NT/2000 server, the master is designated on the Servers tab in the Master Server Properties dialog. To access this dialog, see "Using the Configure - NetBackup Window" on page 57.

2. For detailed troubleshooting information, create a `bpdbm` activity log directory and retry the operation. Then, check the resulting activity log.

Status Code: 229

Message: events out of sequence - image inconsistency

Explanation: A request was made which, if satisfied, would cause the image catalog to become inconsistent.



Recommended Action: Obtain detailed troubleshooting information by creating an activity log directory for `bpdbm`. Then, retry the operation, save the resulting activity log, and call customer support.

Status Code: 230

Message: the specified class does not exist in the configuration database

Explanation: The specified class name does not exist.

Recommended Action: Correct your parameters or options and retry the operation.

Status Code: 231

Message: schedule windows overlap

Explanation: The start and duration times specified for one day of the schedule overlap with another day of the schedule.

Recommended Action: Correct the schedule to eliminate the overlapping backup windows.

Status Code: 232

Message: a protocol error has occurred

Explanation: This is an intermediate status code that usually precedes another status code. It indicates that either the `bpdbm` process (NetBackup Database Manager service on Windows NT/2000) or the process communicating with it has received unexpected information.

Recommended Action: Create an activity log directory for `bpdbm`. Then, retry the operation, save the activity log, and call customer support.

Status Code: 233

Message: premature eof encountered

Explanation: This is an intermediate status code that usually precedes another status code and is associated with a problem in network communication.

Recommended Action: During a restore, this means that `tar` (on the client) received a stream of data that was not what it expected. If this is a new configuration, verify that the tape drive is configured for variable mode (see the *Media Manager Device Configuration Guide*).

If the communication failure is not due to an interrupt on a client system, save all error information and call customer support.

Status Code: 234

Message: communication interrupted

Explanation: This is an intermediate status code that usually precedes another status code and is associated with a problem in network communication. A process, either server or client, received an interrupt signal.

Recommended Action: Save all error information and call customer support.

Status Code: 235

Message: inadequate buffer space

Explanation: This code usually indicates a mismatch between server and client software versions.

Recommended Action:

1. Verify that all NetBackup software is at the same version level. Update earlier versions of NetBackup software.
   - On UNIX NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
   - On Windows NT/2000 NetBackup servers, check the *install_path*`\NetBackup\version.txt` file or the About NetBackup item on the Help menu.
   - On Microsoft Windows clients, check the About NetBackup item on the Help menu.
   - On NetWare target clients, check the Version entry in the `bp.ini` file.

     If the client software is earlier than 3.0, verify that the client is in a Standard type class.
   - On Macintosh clients, check the version file in the `bin` folder in the `NetBackup` folder in the `Preferences` folder.
2. If the problem persists, save all error information and call customer support.

Status Code: 236

Message: the specified client does not exist in an active class within the configuration database

Explanation: A client name was not specified or the specified client does not exist.

Recommended Action: Activate the required class, correct the client name, or add the client to a class that meets your needs. After making the correction, retry the operation.

Status Code: 237

Message: the specified schedule does not exist in an active class in the configuration database

Explanation: The specified schedule does not exist in the NetBackup configuration.

Recommended Action: Activate the required class, correct the schedule name, or create a schedule in a class that meets your needs. After making the correction, retry the operation.

Status Code: 238

Message: the database contains conflicting or erroneous entries

Explanation: The catalog has an inconsistent or corrupted entry.

Recommended Action: Obtain detailed troubleshooting information for `bpdbm` (NetBackup Database Manager service on Windows NT/2000) by creating an activity log directory for it. Then, retry the operation, save resulting activity log, and call customer support.

Status Code: 239

Message: the specified client does not exist in the specified class

Explanation: The specified client is not a member of the specified class.

Recommended Action: Correct the client name specification, specify a different class, or add the required client name to the class. After making the correction, retry the operation.

Status Code: 240

Message: no schedules of the correct type exist in this class

Explanation: The appropriate schedule was not found in the specified class. For example, a user backup specified a class name but no user backup schedule exists in that class.

Recommended Action: Specify a different class or create a schedule of the needed type in the class. After making the correction, retry the operation.

Status Code: 241

Message: the specified schedule is the wrong type for this request

Explanation: The schedule that was specified for an immediate manual backup is not for a full nor an incremental backup. It must be one of these.

Recommended Action: Specify only full or incremental schedules for manual backups. If one does not exist in the class, create one.

Status Code: 242

Message: operation would cause an illegal duplication

Explanation: Processing the request would cause a duplicate catalog entry. This is usually due to a mistake in specifying media IDs for NetBackup catalog backups.

Recommended Action: Check the error reports to determine the specific duplication that would occur. Correct the settings for the operation and retry it.

Status Code: 243

Message: the client is not in the configuration

Explanation: The specified client name was not in the catalog.

Recommended Action: Either correct the client name or add the client to the desired class.

Status Code: 244

Message: main bpsched is already running

Explanation: A `bpsched` process tried to become the main backup scheduler but another process is currently in this mode.

Recommended Action: None.

Status Code: 245

Message: the specified class is not of the correct client type

Explanation: A user backup specified a class that is not the type required for the client.

Recommended Action: Retry the operation by specifying a class that is the correct type for the client. If such a class does not exist, create one.

Status Code: 246

Message: no active classes in the configuration database are of the correct client type

Explanation: A user backup request was not satisfied because no active classes were the type required for the client.

Recommended Action: Create or activate an appropriate class so the user backup request can be satisfied.

Status Code: 247

Message: the specified class is not active

Explanation: Backups for the specified class are disabled because the class is inactive.

Recommended Action: Activate the class and retry the operation.

Status Code: 248

Message: there are no active classes in the configuration database

Explanation: No active class was found that would satisfy the request.

Recommended Action: Activate the appropriate class and retry the operation.

Status Code: 249

Message: the file list is incomplete

Explanation: The server timed out while waiting for the client to finish sending the file list, or a sequencing problem occurred.

Recommended Action: Obtain additional information by first creating activity logs and then attempting to recreate the error. The activity logs to create are as follows:

- On the server, `bptm`, `bpbrm`, and `bpdbm`.
- On UNIX and Windows NT/2000 clients, `bpbkar`.
- On other clients, `bpcd`.

To increase the amount of information included in the logs, see "Activity Logs on PC Clients" on page 66.

Status Code: 250

Message: the image was not created with TIR information

Explanation: This is an internal error and should not be seen by customers.

Recommended Action: Obtain detailed troubleshooting information by creating activity logs for `bptm` and `bpdbm` on the server. Then, retry the operation and check the resulting activity logs.

Status Code: 251

Message: the TIR information is zero length

Explanation: For a true-image backup, the client sent no file information to the master server. NetBackup discovered this condition when it attempted to write the TIR information to media.

Recommended Action:

1. Check the file list for the class and the exclude and include lists on the client to verify that the client has files that are eligible for backup. For example, this status code can appear if the exclude list on the client excludes all files.

2. To obtain detailed troubleshooting information, create activity logs for `bptm` and `bpdbm` on the server. Then, retry the operation and check the resulting activity logs.

Status Code: 254

Message: server name not found in the bp.conf file

Explanation: This error should not occur through normal use of NetBackup.

Recommended Action: Save all error information and call customer support.

Status Code: 500

Message: NB-Java application server not accessible - maximum number of connections exceeded.

Explanation: Indicates that an attempted login failed because the maximum number of NetBackup-Java user services has been achieved. Although the number of allowed user services is very large (>100), it is possible to reach the maximum.

Recommended Action: Ask other users to log off (this limit is not configurable).

Status Code: 501

Message: You are not authorized to use this application.

Explanation: The user is not authorized to use one of the NetBackup Java Administration utilities on the host specified in the login dialog.

Recommended Action: Check the `/usr/openv/java/auth.conf` file on the host specified in the NetBackup-Java login dialog for the proper authorization. If the `auth.conf` file does not exist, it must be created with the proper entry for this user name. Refer to the *NetBackup System Administrator's Guide - UNIX* for more details on the `auth.conf` file.

Status Code: 502

Message: No authorization entry exists in the auth.conf file for username *username*. None of the NB-Java applications are available to that user.

Explanation: The user name is not authorized to use any NetBackup-Java applications on the host specified in the login dialog.

Recommended Action: Check the `/usr/openv/java/auth.conf` file on the machine (host name) specified in the NetBackup-Java login dialog for the proper authorization. If the file does not exist, it must be created with the proper entry for this user name. Refer to the *NetBackup System Administrator's Guide - UNIX* for more details on the `auth.conf` file.

Status Code: 503

Message: Invalid username.

Explanation: For login to a UNIX host, the user name is not recognized by the NetBackup Java application server on the host where the login is requested.

For login to a Windows NT/2000 host, the NetBackup-Java authentication service on the host where the login is requested does not have sufficient privileges for granting the login request.

Recommended Action:

- For UNIX hosts: the user name must be a valid user name in the `passwd` file on the host specified in the login dialog.
- For Windows NT/2000 hosts: refer to the LogonUser function in the section titled "Client/Server Access Control Functions" of the *Windows NT Platform Software Developer's Kit* to determine the required privileges.

Status Code: 504

Message: Incorrect password.

Explanation: For login to a UNIX host, the user name is recognized on the host where the login is requested, but the password supplied is incorrect.

For login to a Windows NT/2000 host, the attempt to log in the user has failed. The failure could be due to an unrecognized user in the specified domain.

Recommended Action:

- Enter the correct password.
- On Windows NT/2000 hosts: The exact error can be found in the `bpjava-msvc` log file. For more details, refer to the LogonUser function in the section "Client/Server Access Control Functions" of the *Windows NT Platform Software Developer's Kit*.

Status Code: 505

Message: Cannot connect to the NB-Java authentication service on the configured port - *configured_port_number*.

Explanation: The initial connection from the NetBackup-Java interface to its authentication service is on the port mentioned in the error message. The port is either being used by another application, or the NetBackup-Java interface and its application server are not configured with the same port. The default port is 13722.

Recommended Action:

1. Compare the `bpjava-msvc` entry in the `/etc/services` file with the `SERVER_PORT` entry in `/usr/openv/java/nbj.conf` file. They must match.

2. Ensure that no other application is using the port configured for the NetBackup-Java interface.

Status Code: 506

Message: Cannot connect to the NB-Java user service on port *port_number*.

Explanation: Once the user name on the login dialog is validated for access by the NetBackup-Java authentication service, a NetBackup-Java user service is used for all other service requests from the NetBackup Administration interface. Communication between the NetBackup-Java interface and user service is attempted on the port number specified in the error message. Refer to the various port configuration options described in the *NetBackup System Administrator's Guide* (UNIX or Windows NT/2000).

On UNIX: the port configuration options are specified in the `/usr/openv/netbackup/bp.conf` file.

On Windows NT/2000: from the NetBackup Administration window, select Configure NetBackup from the Start menu. In the Configure - NetBackup window, select Properties (Read/Write) from the File menu. The General Server tab contains the port options. For more information, refer to the *NetBackup System Administrator's Guide - Windows NT/2000*.

Recommended Action:

1. Restart the NetBackup-Java interface and log in again.

2. If the problem persists, enable detailed activity logging.

3. Restart the NetBackup Java Administration interface and examine the logs.

Status Code: 507

Message: Socket connection to the NB-Java user service has been broken. Please retry your last operation.

Explanation: The connection was broken to the NetBackup Java application server that is running on the NetBackup host you are logged in to.

Recommended Action:

1. Retry the last operation.
2. If the problem persists, restart the NetBackup-Java interface and try again.
3. If the problem still persists, enable detailed activity logging as explained under "Enabling Detailed Activity Logging" on page 74.
4. Restart the NetBackup-Java interface and examine the logs.

Note You may be having network or system problems unrelated to NetBackup.

Status Code: 508

Message: Cannot write file.

Explanation: This error is caused by one of the following:

- The NetBackup-Java user service has attempted to write to a file that does not have write permissions. The solution is to enable write privileges.
- The NetBackup-Java user service has attempted to write to a temporary file whose unique name cannot be constructed. This condition is unlikely, but could result from an exhaustion of system resources (from the filling of the name space).

Recommended Action: The specific details may be retrieved from the user service log files. Enable detailed activity logging as explained under "Enabling Detailed Activity Logging**" on page 74**.

Status Code: 509

Message: Cannot execute program.

Explanation: The NetBackup-Java authentication or user service has reported an error relating to the creation (or demise) of a child job process. The NetBackup-Java service programs create separate jobs to accomplish specific tasks, as follows. The NetBackup-Java authentication service creates the NetBackup-Java user service. Upon successful creation of and connection to the NetBackup-Java user service, all other child processes are created by the NetBackup-Java user service on behalf of requests made by the NetBackup-Java interface.

The cause of status code 509 can be found in the appropriate log file, either for `bpjava-msvc` or `bpjava-usvc`. The cause can be categorized as one of the following:

- A job (started by either the NetBackup-Java authentication service or user service) no longer exists, and did not report its result status.

- A job (started by either the NetBackup-Java authentication service or user service) cannot be monitored by the NetBackup-Java service. This is probably due to a lack of system resources (insufficient memory).
- The maximum number of non-transient activity monitor jobs (>100) have already been started.

Recommended Action:

1. If the problem persists, restart the NetBackup-Java interface and try again.
2. If the problem still persists, enable detailed activity logging as explained under "Enabling Detailed Activity Logging" on page 74.
3. Restart the NetBackup-Java interface and examine the logs.

Note The error is probably the result of a system resource issue. When detailed activity logging has been enabled, the details may be retrieved from the `bpjava-msvc` or `bpjava-usvc` log files.

Status Code: 510

Message: File already exists: *file_name*

Explanation: The NetBackup-Java user service has attempted to create a file that already exists.

Recommended Action: Remove the file, which can be identified in the user service log files. Refer to "Troubleshooting the Java Administration Interface" on page 72.

Status Code: 511

Message: NB-Java application server interface error: *Java exception*

Explanation: This is a generic error for all non-socket IO/connection-broken related errors (status code 507) that could occur when processing the data from the NetBackup-Java authentication or user services. The Java exception will provide some additional detail about the error.

This error usually results from system or network problems.

Recommended Action:

1. If the problem persists, restart the NetBackup-Java interface and try again.
2. If the problem still persists, enable detailed activity logging as explained under "Enabling Detailed Activity Logging" on page 74.

3. Restart the NetBackup-Java interface and examine the logs.

Note The error is probably the result of a system resource issue. When detailed activity logging has been enabled, the details may be retrieved from the `bpjava-msvc` or `bpjava-usvc` log files.

Status Code: 512

Message: Internal error - a bad status packet was returned by NB-Java application server that did not contain an exit status code.

Explanation: The NetBackup-Java authentication or user service returned a data packet indicating an error, but no status code or error message was contained within it.

Recommended Action:

1. If the problem persists, restart the NetBackup-Java interface and try again.
2. If the problem still persists, enable detailed activity logging as explained under "Enabling Detailed Activity Logging" on page 74.
3. Restart the NetBackup-Java interface and examine the logs.

Note The error is probably the result of a system resource issue. When detailed activity logging has been enabled, the details may be retrieved from the `bpjava-msvc` or `bpjava-usvc` log files.

Status Code: 513

Message: bpjava-msvc: the client is not compatible with this server version (*server_version*).

Explanation: The NetBackup-Java application server (on the remote host you are logging in to) is not the same version as the NetBackup-Java interface on your local host. The two are therefore incompatible.

Recommended Action:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either the machine specified in the login dialog or on the local host where you started the NetBackup Java interface.

Status Code: 514

Message: NB-Java: bpjava-msvc is not compatible with this application version (*application_version*). You may try login to a different NetBackup host or exit the application. The remote NetBackup host will have to be configured with the same version of NetBackup as the host you started the application on.

Explanation: The NetBackup-Java application server (on the remote host you are logging in to) is not the same version as the NetBackup-Java interface on your local host. The two are therefore incompatible.

Recommended Action:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either the machine specified in the login dialog or on the local host where you started the NetBackup Java interface.

Messages

This section lists the NetBackup error messages alphabetically. The status code is included in parentheses after the message. Refer to the previous list of status codes for explanations and recommended actions.

/usr/openv/netbackup/bp.conf not found

(Status Code 110)

a protocol error has occurred

(Status Code 232)

access to server backup restore manager denied

(Status Code 206)

access to the client was not allowed

(Status Code 59)

afs/dfs command failed

(Status Code 78)

allocation failed

(Status Code 10)

an entry in the filelist expanded to too many characters

(Status Code 70)

an extension package is needed but was not installed

(Status Code 9)

an invalid entry was encountered

(Status Code 223)

another NB database backup is already in progress

(Status Code 125)

archive file removal failed

(Status Code 4)

authentication failed

(Status Code 160)

Auspex SP/Backup failure

(Status Code 88)

Backup Exec operation failed

(Status Code 151)

backup restore manager failed to read the file list

(Status Code 53)

backups are not allowed to span media

(Status Code 166)

bpjava-msvc: the client is not compatible with this server version (*server_version*)

(Status Code 513)

bpstart_notify failed

(Status Code 73)

can't connect to client

(Status Code 58)

cannot connect on socket

(Status Code 25)

cannot connect to server backup restore manager

(Status Code 205)

Cannot connect to the NB-Java authentication service on the configured port - *configured_port_number*

(Status Code 505)

Cannot connect to the NB-Java user service on port *port_number*

(Status Code 506)

Cannot execute program

(Status Code 509)

cannot find configuration database record for requested NB database backup

(Status Code 120)

cannot find requested volume pool in Media Manager volume database

(Status Code 167)

cannot get a bound socket

(Status Code 146)

cannot make required directory

(Status Code 35)

cannot overwrite media, data on it is protected

(Status Code 168)

cannot perform specified media import operation

(Status Code 176)

cannot position to correct image

(Status Code 94)

cannot read backup header, media may be corrupted

(Status Code 173)

cannot read media header, may not be NetBackup media or is corrupted

(Status Code 172)

Cannot write file

(Status Code 508)

child process killed by signal

(Status Code 27)

client backup failed to read the file list

(Status Code 67)

client backup failed to receive the CONTINUE BACKUP message

(Status Code 66)

client backup was not attempted

(Status Code 195)

client backup was not attempted because backup window closed

(Status Code 196)

client cannot read the mount table

(Status Code 60)

client connection refused

(Status Code 57)

client did not start

(Status Code 49)

client hostname could not be found

(Status Code 48)

client is not validated to perform the requested operation

(Status Code 135)

client is not validated to use the server

(Status Code 131)

client name mismatch

(Status Code 39)

client process aborted

(Status Code 50)

client timed out waiting for bpend_notify to complete

(Status Code 75)

client timed out waiting for bpstart_notify to complete

(Status Code 74)

client timed out waiting for the continue message from the media manager

(Status Code 65)

client timed out waiting for the file list

(Status Code 68)

client's network is unreachable

(Status Code 56)

client/server handshaking failed

(Status Code 26)

communication interrupted

(Status Code 234)

connection refused by server backup restore manager

(Status Code 204)

continue

(Status Code 221)

could not deassign media due to Media Manager error

(Status Code 177)

could not get group information

(Status Code 38)

could not get passwd information

(Status Code 30)

could not set group id for process

(Status Code 32)

could not set user id for process

(Status Code 31)

daemon fork failed

(Status Code 148)

daemon is already running

(Status Code 145)

database system error

(Status Code 220)

density is incorrect for the media id

(Status Code 179)

done

(Status Code 222)

error creating or getting message queue

(Status Code 209)

error obtaining date of last backup for client

(Status Code 207)

error receiving information on message queue

(Status Code 210)

error requesting media (tpreq)

(Status Code 98)

error sending information on message queue

(Status Code 212)

evaluation software has expired. See www.veritas.com for ordering information

(Status Code 161)

events out of sequence - image inconsistency

(Status Code 229)

execution of the specified system command returned a nonzero status

(Status Code 77)

failed accessing daemon lock file

(Status Code 158)

failed closing mail pipe

(Status Code 102)

failed opening mail pipe

(Status Code 101)

failed reading class database information

(Status Code 218)

failed reading global config database information

(Status Code 215)

failed reading retention database information

(Status Code 216)

failed reading storage unit database information

(Status Code 217)

failed reading user directed filelist

(Status Code 208)

failed trying to allocate memory
(Status Code 36)

failed trying to exec a command
(Status Code 29)

failed trying to fork a process
(Status Code 28)

failed waiting for child process
(Status Code 34)

failed while trying to send mail
(Status Code 33)

fatal NB media database error
(Status Code 91)

File already exists: *file_name*
(Status Code 510)

file close failed
(Status Code 15)

file does not exist
(Status Code 142)

file open failed
(Status Code 12)

file path specified is not absolute
(Status Code 141)

file pathname exceeds the maximum length allowed

(Status Code 105)

file read failed

(Status Code 13)

file write failed

(Status Code 14)

found no images or media matching the selection criteria

(Status Code 190)

getservbyname failed

(Status Code 19)

handshaking failed with server backup restore manager

(Status Code 201)

host is unreachable

(Status Code 47)

inadequate buffer space

(Status Code 235)

Incorrect password

(Status Code 504)

Internal error - a bad status packet was returned by NB-Java application server that did not contain an exit status code

(Status Code 512)

invalid command parameter

(Status Code 20)

invalid command protocol

(Status Code 143)

invalid command usage

(Status Code 144)

invalid file pathname found, cannot process request

(Status Code 106)

invalid filelist specification

(Status Code 69)

invalid request

(Status Code 133)

Invalid username

(Status Code 503)

licensed use has been exceeded

(Status Code 159)

main bpsched is already running

(Status Code 244)

media close error

(Status Code 87)

media id is either expired or will exceed maximum mounts

(Status Code 169)

media id is not in NetBackup volume pool

(Status Code 178)

media id must be 6 or less characters

(Status Code 171)

Media Manager device daemon (ltid) is not active

(Status Code 80)

Media Manager volume daemon (vmd) is not active

(Status Code 81)

media manager detected image that was not in tar format

(Status Code 92)

media manager found wrong tape in drive

(Status Code 93)

media manager killed by signal

(Status Code 82)

media manager received no data for backup image

(Status Code 90)

media manager - system error occurred

(Status Code 174)

media open error

(Status Code 83)

media position error

(Status Code 86)

media read error

(Status Code 85)

media write error

(Status Code 84)

NB database backup failed, a path was not found or is inaccessible

(Status Code 124)

NB database backup header is too large, too many paths specified

(Status Code 126)

NB image database contains no image fragments for requested backup id/copy number

(Status Code 165)

NB-Java application server interface error: *Java exception*

(Status Code 511)

NB-Java application server not accessible - maximum number of connections exceeded

(Status Code 500)

NB-Java: bpjava-msvc is not compatible with this application version (*application_version*). You may try login to a different NetBackup host or exit the application. The remote NetBackup host will have to be configured with the same version of NetBackup as the host you started the application on.

(Status Code 514)

NDMP backup failure

(Status Code 99)

network connection broken

(Status Code 40)

network connection timed out

(Status Code 41)

network read failed

(Status Code 42)

network write failed

(Status Code 44)

no active classes contain schedules of the requested type for this client

(Status Code 198)

no active classes in the configuration database are of the correct client type

(Status Code 246)

No authorization entry exists in the auth.conf file for username *username*. None of the NB-Java applications are available to you.

(Status Code 502)

no entity was found

(Status Code 227)

no files specified in the file list

(Status Code 112)

no images were successfully processed

(Status Code 191)

no media is defined for the requested NB database backup

(Status Code 121)

no schedules of the correct type exist in this class

(Status Code 240)

no storage units available for use

(Status Code 213)

none of the files in the file list exist

(Status Code 71)

none of the requested files were backed up

(Status Code 2)

not all requested files were restored

(Status Code 175)

operation not allowed during this time period

(Status Code 199)

operation requested by an invalid server

(Status Code 37)

operation would cause an illegal duplication

(Status Code 242)

permission denied by client during rcmd

(Status Code 55)

pipe close failed

(Status Code 18)

premature eof encountered

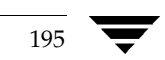
(Status Code 233)

process was killed by a signal

(Status Code 63)

regular bpsched is already running

(Status Code 214)



request attempted on a non reserved port

(Status Code 45)

requested media id is in use, cannot process request

(Status Code 97)

requested media id was not found in NB media database and/or MM volume database

(Status Code 95)

required or specified copy was not found

(Status Code 147)

required value not set

(Status Code 152)

schedule windows overlap

(Status Code 231)

scheduler child killed by signal

(Status Code 211)

scheduler found no backups due to run

(Status Code 200)

server backup restore manager's network is unreachable

(Status Code 203)

server is not the master server

(Status Code 153)

server name not found in the bp.conf file

(Status Code 254)

server not allowed access

(Status Code 46)

SERVER was not specified in /usr/openv/netbackup/bp.conf

(Status Code 111)

socket close failed

(Status Code 22)

Socket connection to the NB-Java user service has been broken. Please retry your last operation.

(Status Code 507)

socket open failed

(Status Code 21)

socket read failed

(Status Code 23)

socket write failed

(Status Code 24)

specified device path does not exist

(Status Code 122)

specified disk path is not a directory

(Status Code 123)

specified media or path does not contain a valid NB database backup header

(Status Code 127)

storage unit characteristics mismatched to request

(Status Code 154)

system call failed

(Status Code 11)

system error occurred

(Status Code 130)

system error occurred while processing user command

(Status Code 100)

tar did not find all the files to be restored

(Status Code 185)

tar had an unexpected error

(Status Code 184)

tar received an invalid archive

(Status Code 183)

tar received an invalid argument

(Status Code 181)

tar received an invalid file name

(Status Code 182)

tar received no data

(Status Code 186)

tar was successful

(Status Code 180)

termination requested by administrator

(Status Code 150)

text exceeded allowed length

(Status Code 225)

the archive failed to back up the requested files

(Status Code 7)

the backup failed to back up the requested files

(Status Code 6)

the client is not in the configuration

(Status Code 243)

the client type is incorrect in the configuration database

(Status Code 72)

the database contains conflicting or erroneous entries

(Status Code 238)

the entity already exists

(Status Code 226)

the file list is incomplete

(Status Code 249)

the image was not created with TIR information

(Status Code 250)

the maximum number of jobs per client is set to 0

(Status Code 194)

the requested operation was partially successful

(Status Code 1)

the requested operation was successfully completed

(Status Code 0)

the required storage unit is unavailable

(Status Code 219)

the restore failed to recover the requested files

(Status Code 5)

the server is not allowed to write to the client's filesystems

(Status Code 189)

the specified class does not exist in the configuration database

(Status Code 230)

the specified class is not active

(Status Code 247)

the specified class is not of the correct client type

(Status Code 245)

the specified client does not exist in an active class within the configuration database

(Status Code 236)

the specified client does not exist in the specified class

(Status Code 239)

the specified schedule does not exist in an active class in the configuration database

(Status Code 237)

the specified schedule does not exist in the specified class

(Status Code 197)

the specified schedule is the wrong type for this request

(Status Code 241)

the TIR information is zero length

(Status Code 251)

there are no active classes in the configuration database

(Status Code 248)

there was a conflicting specification

(Status Code 224)

timed out connecting to client

(Status Code 54)

timed out connecting to server backup restore manager

(Status Code 202)

timed out waiting for database information

(Status Code 51)

timed out waiting for media manager to mount volume

(Status Code 52)

timed out waiting for the client backup to start

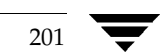
(Status Code 64)

unable to allocate new media for backup, storage unit has none available

(Status Code 96)

unable to determine the status of rbak

(Status Code 8)



unable to mount media because its in a DOWN drive or misplaced

(Status Code 164)

unable to process request

(Status Code 228)

unexpected message received

(Status Code 43)

unimplemented feature

(Status Code 16)

user id was not superuser

(Status Code 140)

valid archive image produced, but no files deleted due to non-fatal problems

(Status Code 3)

wbak exited abnormally

(Status Code 62)

wbak was killed

(Status Code 61)

You are not authorized to use this application

(Status Code 501)

Disaster Recovery 5

This chapter has procedures for recovering your data in case of a server or client disk failure. The recovery procedures are as follows:

- Master Server Disk Recovery
- Media Server Disk Recovery
- Client System Disk Recovery - UNIX
- Client System Disk Recovery - Windows NT/2000, 98, 95
- Recovering the NetBackup Databases

Master Server Disk Recovery

The procedures in this section explain how to recover your data if the system disk fails on a UNIX master server. Two general cases are considered:

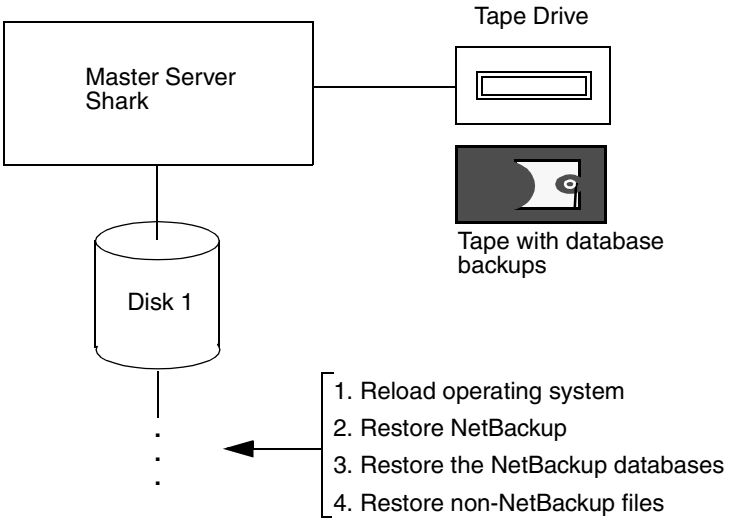
- Root file system is intact. The operating system, NetBackup software, and some (if not all) other files are assumed to be lost.
- Root file system is lost along with everything else on the disk. This is a total recovery.

In both cases, you restore the server to the state it was in at the time of the most recent back up of the NetBackup databases. If the recovery is successful, reconfiguration is unnecessary.

Recovering Master Server When Root is Intact

The general steps are to first restore the operating system, then restore NetBackup, and finally to restore all other files (Figure 1).

Figure 1. Recover Master Server - Root Intact (overview)



1. Verify that the operating system is working. If it isn't, take the appropriate corrective actions.

2. Reinstall NetBackup software. Do not configure NetBackup classes or devices.

   See the *NetBackup Installation Guide - UNIX* for instructions.

3. Recover the NetBackup databases by using the `bprecover` command on the master server.

   Choose one of the procedures under "Recovering the NetBackup Databases" on page 211.

Caution In step 4, do not restore files to the `/usr/openv/netbackup/db` or `/usr/openv/volmgr/database` directories. These directories were recovered in step 3 and overwriting them with regular backups will leave the databases in an inconsistent state.

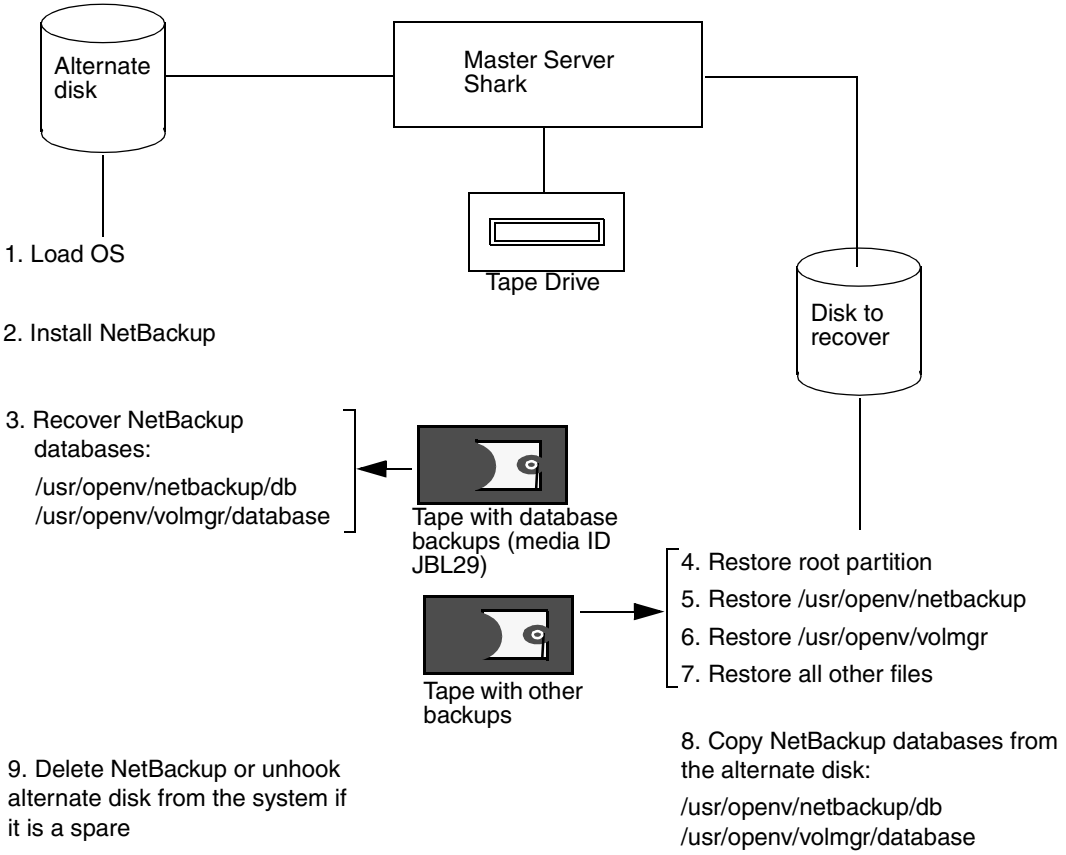
4. Start the NetBackup client-user interface and restore other files to the server as desired.

Recovering Master Server When Root is Lost

This procedure assumes that the root file system has been lost along with all other files on the system disk. Figure 2 illustrates the procedure.

The recovery method described here reloads the operating system on an alternate boot disk and boots from this disk during the recovery. This lets you recover the root partition without risking a crash due to overwriting files that are being used by the operating system during the restore.

Figure 2. Recover Master Server When Root is Lost (overview)



1. Load the operating system on the alternate boot disk, using the same procedure as you normally would for the server.

2. Create, on the alternate disk, the partition and directory where NetBackup and its databases resided on the original disk. By default, they reside under `/usr`.

3. Install NetBackup on the alternate disk. See the *NetBackup Installation Guide - UNIX* for instructions on installing NetBackup software.

Note Do not reconfigure NetBackup classes. If reconfiguration is necessary, you will be given the necessary instructions later in this procedure.

Install only the robotic software for the devices that are required to read backups of the NetBackup databases and the regular backups of the disk being restored. If a nonrobotic drive can read these backups, then you do not need a robot. The example on Figure 2 requires only a nonrobotic tape drive.

4. Recover the NetBackup databases to the alternate disk by using the `bprecover` command on the master server.

   The NetBackup databases can be recovered only to the same location from which they were backed up (alternate path recovery is not allowed).

   Choose one of the procedures under "Recovering the NetBackup Databases" on page 211.

5. Restore the root partition to the disk you are recovering.

6. Start the NetBackup client user interface and restore the latest backed up version of all files to the disk you are recovering.

   It is not necessary to restore the NetBackup databases because you will be doing this in step 7. But you must restore all other NetBackup files.

7. Copy the NetBackup databases from the alternate disk to the disk that you are recovering. These are the databases recovered in step 4.

8. Stop all NetBackup processes that you started from NetBackup on the alternate disk.

9. Start and test the copy of NetBackup on the disk that you have recovered.

   Try the NetBackup Administration utilities. Also, try some backups and restores.

10. When you are satisfied that the recovery is complete, delete the NetBackup files from the alternate disk. Or, unhook that disk, if it is a spare.

11. Make the recovered disk the boot disk again.

Media Server Disk Recovery

Note The term *media server*, as distinct from *master server* or *server*, does not apply to the NetBackup BusinesServer product. When troubleshooting a BusinesServer installation, please ignore any references to media server.

The procedure for recovering a media server where the system disk has failed is the same as for a master server, except that you use the following paths when running `bprecover`:

If the media server is a UNIX system:

media_server_name:`/usr/openv/netbackup/db/media`

media_server_name:`/usr/openv/volmgr/database`

If the media server is a Windows NT/2000 system:

media_server_name:*install_path*`\NetBackup\db\media`

media_server_name:*install_path*`\Volmgr\database`

In the above paths, substitute the host name of the media server for *media_server_name* (for example, elk). For *install_path*, substitute the directory where NetBackup is installed.

You can execute `bprecover` from either the master or media server by specifying the correct destination host with the `bprecover -dhost` option.

Client System Disk Recovery - UNIX

The procedure for recovering the system disk on a client workstation is as follows:

1. Reload the operating system the way you normally would for a client workstation of that type.

Note If the root file system is lost, the best approach may be to reload the operating system on an alternate boot disk and boot from this disk. After you restore NetBackup, you can restore root to its original partition. This lets you recover the root partition without risking a crash due to overwriting files being used by the operating system during the restore. The procedure is similar to that for the master server, except you do not have to install Media Manager or recover the NetBackup databases. (see “Recovering Master Server When Root is Lost” on page 205).

2. Reinstall NetBackup client software.

3. Use the client-user interface to select and restore files.

Client System Disk Recovery - Windows NT/2000, 98, 95

The following procedure explains how to perform a total recovery of a Windows NT/2000, 98, or 95 NetBackup client in the event of a system disk failure.

Note For Windows NT/2000 systems: if you have installed and configured NetBackup Intelligent Disaster Recovery, refer to the *NetBackup System Administration Guide* instead of the instructions below.

This procedure assumes that the Windows operating system and NetBackup must be reinstalled in order to boot the system and perform a restore.

Assumptions

- The NetBackup client was running one of the following:
  - Windows NT Server or Workstation 4.0 or above, or Windows 2000.
  - Windows 98 or 95 software
- The NetBackup client was backed up with version 3.0 or later NetBackup client and server software.
- The NetBackup master server to which the client sent its backups is operational. This is the server from which you will be requesting the restore.
- The backups included the directory where the operating system and therefore the registry resided (typically `C:\winnt40` on Windows NT and `C:\Windows` on Windows 98 or 95).

  If the backups excluded any files that resided in the above directory, it is possible that you will not be able to restore the system so it completely matches its previous configuration.
- Defective hardware has been replaced.

Before Starting

Verify that you have the following:

- Windows NT/2000, 98, or 95 system software to reinstall on the NetBackup client that is being restored:
  - Reinstall the same type and version of software that was previously used. For example, do not install Windows NT Server 4.0 software if, before the failure, the system was a Windows NT 4.0 workstation.
  - For a Windows NT/2000 client, this software must be Windows NT Server or Workstation 4.0 or above, or Windows 2000.

- NetBackup 3.0 or later client software to install on the client that is being restored.
- Special drivers or other software required to get the hardware operational (for example, a special driver for the disk drive).
- IP address and host name of the NetBackup client.
- IP address and host name of the NetBackup master server.
- Partitioning and formatting scheme that was used on the system that you are restoring. You must duplicate that scheme during Windows NT/2000, 98, or 95 installation.

To Recover a Windows NT/2000, 98, or 95 Client Disk

1. Install a minimal Windows NT/2000, 98, or 95 operating system (perform the Express install).

   During the install, be certain to:

   - Partition the disk as it was before the failure (if partitioning is necessary). Then, reformat each partition as it was before the failure.
   - Install the operating system in the same partition that was used before the failure.
   - Specify the default workgroup. Do not restore to the domain.
   - Follow any hardware manufacturers instructions that apply, such as loading SSD on a Compaq system.

2. Reboot the system when the install is complete.

3. Configure the NetBackup client system to re-establish network connectivity to the NetBackup master server.

   For example, if your network uses DNS, the configuration on the client must use the same IP address as before the failure and must specify the same name server (or another name server that recognizes both the NetBackup client and master server). On the client, configure DNS in the Network dialog box that you access from the Control Panel.

4. Install NetBackup client software.

   Refer to the *NetBackup Installation Guide - PC Clients* for instructions. Ensure that you specify the correct names for the client and master server. To specify the client name, start the user interface on the client and click Configure on the Actions menu. Enter the client name on the General tab of the NetBackup Configuration dialog. To specify the server name, click Specify NetBackup Machines on the Actions menu and make the entry on the Servers tab.

5. Enable debug logging by creating the following debug log directories on the client:

   On a Windows NT/2000 client:

   install_path\NetBackup\Logs\tar

   install_path\NetBackup\Logs\bpinetd

   On a Windows 98 or 95 client:

   install_path\NetBackup\Logs\bpcd

   NetBackup creates logs in these directories.

6. For a Windows NT/2000 client, stop and restart the NetBackup Client Manager service.

   This enables NetBackup to start logging to the bpinetd debug log.

7. For a Windows 98 or 95 client, stop and restart the NetBackup Client Daemon.

   This enables NetBackup to start logging to the bpcd debug log.

8. Use the NetBackup client user interface to restore the system and user files to the client system.

   For example, if all files are on the C: drive, restoring that drive restores the entire system.

   To restore files, you do not have to be the administrator, but you must have restore privileges. For example, on Windows NT/2000, you must be a member of the Restore group, which is one of the built-in Windows NT/2000 groups. Refer to the online help or *NetBackup User's Guide - Microsoft Windows* for instructions on how to restore files.

Note NetBackup restores the registry when it restores the Windows NT/2000, 98, or Windows 95 system files. For example on a Windows NT/2000 client, if the system files are in the C:\Winnt40 directory, NetBackup restores the registry when it restores that directory and all its subordinate subdirectories and files.

9. Check for ERR or WRN messages in the log files that are in the directories you created in step 5.

   - For a Windows NT/2000 client, these are the tar and inetd log files.
   - For a Windows 98 or 95 client, this is the bpcd log file.

   If the logs indicate problems with the restore of Windows NT/2000, 98, or Windows 95 operating system files, resolve those problems before proceeding.

10. Reboot the NetBackup client system.

When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

Recommended Backup Practices

In addition to backing up files on a regular basis it is important to select the correct files to back up. The first concern is to include all files with records that are critical to users and the organization. It is equally important to back up system and application files, so you can quickly and accurately restore a system to normal operation if a disaster occurs.

Include all Windows NT/2000, 98, and 95 system files in your backups. For example, if Windows NT/2000 is installed in the `C:\Winnt40` directory, include this directory in the list of those that you are backing up (it may be best to back up the entire drive). In addition to the other system software, the Windows NT/2000, 98, and 95 system directories include the registry, without which it is impossible to restore the client to its original configuration. If you are using a NetBackup exclude list for a client, do not specify any Windows NT/2000, 98, or 95 system files in that list.

It is not a good idea to omit executable and other files for applications such as NetBackup. It is tempting to save tape by excluding these easy to reinstall files. However, backing up the entire application, ensures that you can restore it to its exact configuration. For example, if you have applied software updates or patches, restoring from a backup eliminates the need to reapply them, thus reducing recovery time.

For information on how to configure scheduled backups, see the *NetBackup System Administrator's Guide*. For instructions on performing user backups and archives, see the *NetBackup User's Guide - Microsoft Windows*.

Recovering the NetBackup Databases

The NetBackup databases contain critical information and must be recovered before any other backups.

Master servers have the following NetBackup database files:

```
/usr/openv/netbackup/db
/usr/openv/volmgr/database
```

Media servers have the following NetBackup database files:

- UNIX NetBackup media server:

  ```
  /usr/openv/netbackup/db/media
  /usr/openv/volmgr/database
  ```

- Windows NT/2000 NetBackup media server:

install_path\netbackup\db\media

install_path\volmgr\database

For *install_path*, substitute the directory where NetBackup and Media Manager are installed (C:\VERITAS by default).

Because of their importance, the databases are backed up separately from other files as described in the *NetBackup System Administrator's Guide - UNIX*. To recover the databases, use the bprecover command:

/usr/openv/netbackup/bin/admincmd/bprecover

The topics in this section explain how to use bprecover to recover NetBackup database backups. Also, see the description in the NetBackup Commands appendix in the *NetBackup System Administrator's Guide - UNIX.*

Note The following discussions assume that NetBackup has been reinstalled, if required. (See "Master Server Disk Recovery" on page 203.)

Identifying the Most Recent Database Backup

Caution Before you can recover the NetBackup databases, you must know which media ID has their latest backups. Without this media ID, you cannot accurately recover your databases and your only option is to use the NetBackup import feature to import all lost backup records into your NetBackup databases (see the *NetBackup System Administrator's Guide - UNIX*).

As mentioned in the *NetBackup System Administrator's Guide - UNIX*, the best way to track media IDs for database backups is to configure E-mail notifications with the E-mail Address global attribute. This attribute causes NetBackup to specify the status and media ID in an E-mail to the administrator each time a database backup occurs. You can then check the E-mail to determine the last media ID used.

If you know the media IDs that were used but are not sure which of them has the most recent backup, use the -l option of bprecover to list the backups on each media ID. This information includes the date and time that the media was written.

Example 1: List by Using a Raw Device

Assume the database backup was to tape but the Media Manager part of the databases was lost so Media Manager cannot control the drive.

Note If the /dev file for the device you will use for listing the database information is lost in the failure, you must create the special device file path for that device before using bprecover. See the *Media Manager Device Configuration Guide* for information on creating this path.

In this case, insert the media in an appropriate drive (assume the raw-device path is /dev/rmt/hc2d4). Then, execute the following command on the NetBackup server that has the drive.

```
bprecover -l -tpath /dev/rmt/hc2d4
Database Backup Information from /dev/rmt/hc2d4
Created:      03/30/93 11:31:34
Server:       bphost
Block size:   32768
        Path
        ----
IMAGE1 /usr/openv/netbackup/db
IMAGE2 /usr/openv/volmgr/database
```

Example 2: List by Using a Media Manager Controlled Drive

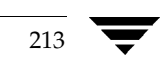
Assume the Media Manager part of the databases is intact and the backup was done to an 8 mm tape with media ID JBL29. Insert the tape into an appropriate drive. Then, execute the following bprecover command on the NetBackup server that has the drive (the Media Manager device daemon, ltid, must be active).

```
bprecover -l -ev JBL29 -d 8mm
Database Backup Information from JBL29
Created:      04/02/93 05:50:51
Server:       bphost
Block size:   32768
        Path
        ----
IMAGE1 /usr/openv/netbackup/db
IMAGE2 /usr/openv/volmgr/database
```

Example 3: List Disk Path

Assume the database backup was done to disk path /disk1/bpbackup and this disk has not failed. Assuming NetBackup is installed and operating, execute the following bprecover command to list the backup information.

```
bprecover -l -dpath /disk1/bpbackup
Database Backup Information from /disk1/bpbackup
Created:      03/30/93 11:31:34
Server:       bphost
       Path
```

```
       ----
IMAGE1 /usr/openv/netbackup/db
IMAGE2 /usr/openv/volmgr/database
```

Example 4: Media Server

Assume the master server is a UNIX system with no tape drives and the media server is a Windows NT/2000 system with a 4 mm tape drive. The database backup was done to the 4 mm tape drive on the Windows NT/2000 media server.

Here, we mount the media in the appropriate drive (assume the raw device path is `\\.\Tape0`) and execute the following `bprecover` command on the media server.

```
bprecover -l -tpath \\.\Tape0
Database Backup Information from \\.\Tape0

Created:      03/31/97 11:31:34
Server:       nbmedia
Block Size:   32768

         Path
         ----
IMAGE1 nbmaster:/usr/openv/netbackup/db
IMAGE2 nbmaster:/usr/openv/volmgr/database
IMAGE3 nbmedia:C:\VERITAS\NetBackup\db\media
IMAGE4 nbmedia:C:\VERITAS\Volmgr\database
```

Procedures for Recovering NetBackup Databases

This section explains how to recover the NetBackup databases when all or part of them are lost. You perform this recovery with the `bprecover` command.

The method required to recover the databases depends on:

- The type of media that contains the backup of the NetBackup databases (tape, optical, or magnetic disk).

  and

- Whether the Media Manager part of those databases is still intact. The Media Manager database files are normally in the `/usr/openv/volmgr/database` directory.

Note The Media Manager device databases are binary files and you cannot restore them to a different type of platform.

Before Starting

- Reinstall the NetBackup software (if necessary) as explained in "Master Server Disk Recovery" on page 203 or "Media Server Disk Recovery" on page 207.
- If you had created symbolic links to the database locations, be sure to manually recreate those links before starting the recovery.
- Find the tape that has the latest database backups.
- Ensure that the disk where you are restoring the databases contains the directory where the databases resided.

  This is required because the `bprecover` command always restores the NetBackup databases to the path from which they were backed up (alternate-path restores are not allowed).

Recover DB From Tape or Optical - Media Manager DB Lost

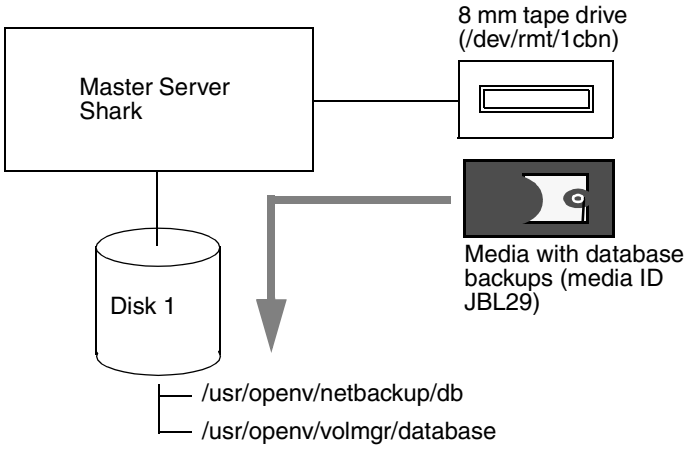
If the latest NetBackup database backup is on tape or optical disk and the Media Manager database files are lost, specify a raw-device path on the `bprecover` command. This method involves mounting the backup media in a drive and using the `-tpath` or `-opath` parameter.

Note If the `/dev` file was lost for the device you are using to recover the databases, create the special device file path for that device before using `bprecover`. See the *Media Manager Device Configuration Guide* for information on creating this path.

1. Insert the database backup media into an appropriate drive.

   The example on Figure 3 shows a nonrobotic tape drive connected to a NetBackup master server.

Figure 3. Recover Databases to Same Disk - UNIX



2. Stop the NetBackup request daemon (`bprd`) and NetBackup database manager daemon (`bpdbm`).

   - Stop `bprd` by using the Terminate Request Daemon command on the `bpadm` Special Actions menu (or `xbpadm` File menu).
   - Stop `bpdbm` by executing:

     `/usr/openv/netbackup/bin/bpdbm -terminate`

3. Stop the Media Manager device daemon (`ltid`) and Media Manager volume daemon (`vmd`).

   - Stop `ltid` with the following command:

     `/usr/openv/volmgr/bin/stopltid`

- Stop `vmd` by executing **`/usr/openv/volmgr/bin/vmctrldbm -t`** (or use Terminate Media Manager volume Daemon command on the `xvmadm` File menu).

4. On the NetBackup server where the drive attaches, execute the `bprecover` command to recover the required files and directories. Specify the raw-device path for the drive where you inserted the media in step 1.

   Example 1

   The following command interactively restores images to disk 1 on Figure 3 by using raw device path `/dev/rmt/1cbn`:

   ```
   bprecover -r -tpath /dev/rmt/1cbn
   Recover shark:/usr/openv/netbackup/db y/n (n)? y
   Recovering shark:/usr/openv/netbackup/db
   ```

```
Recover shark:/usr/openv/volmgr/database y/n (n)? y
Recovering shark:/usr/openv/volmgr/database
```

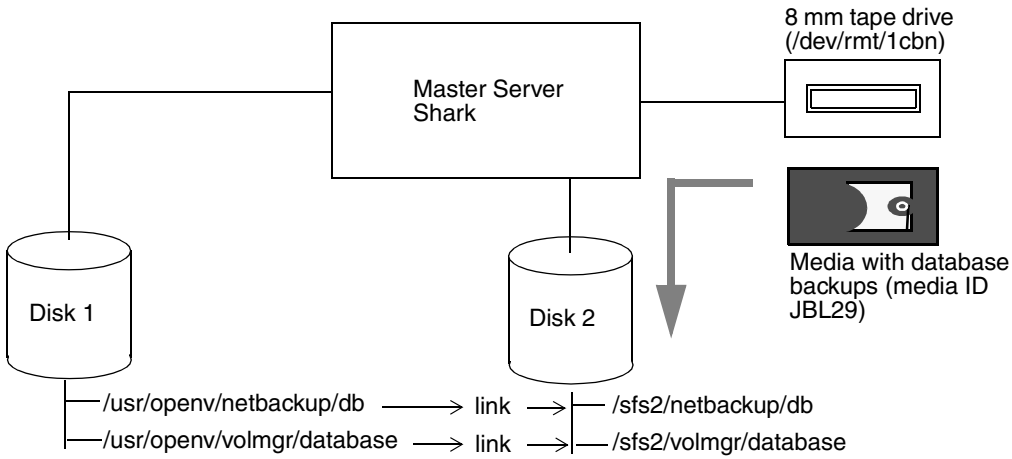
Example 2

If the databases were backed up from another disk, `bprecover` restores them to that disk:

```
bprecover -r -tpath /dev/rmt/1cbn
Recover shark:/sfs2/netbackup/db y/n (n)? y
Recovering shark:/sfs2/netbackup/db
Recover shark:/sfs2/volmgr/database y/n (n)? y
Recovering shark:/sfs2/volmgr/database
```

Figure 4 shows links from the NetBackup database directories on disk 1 to the actual database location on disk 2. You must manually recreate these links if they are lost.

Figure 4. Recover Databases to Another Disk



Example 3

If you have media servers, `bprecover` includes their database paths in the prompts and you select the databases you want to recover.

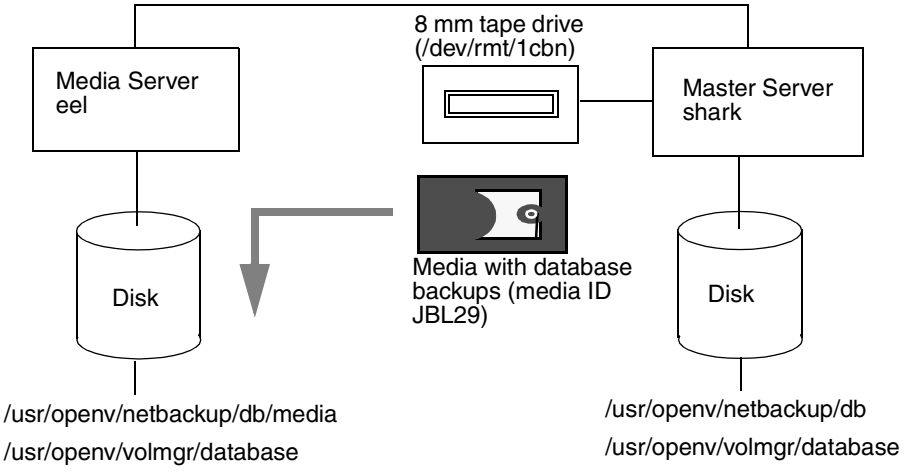
The following example recovers only the databases for a UNIX media server named eel (see Figure 5). Here, you execute `bprecover` on the UNIX master server shark and use the `-dhost` option to specify eel as the destination host:

```
bprecover -r -tpath /dev/rmt/1cbn -dhost eel
Recover shark:/usr/openv/netbackup/db y/n (n)? n
Recover shark:/usr/openv/volmgr/database y/n (n)? n
Recover eel:/usr/openv/netbackup/db/media y/n (n)? y
```

```
Recovering eel:/usr/openv/netbackup/db/media
Recover eel:/usr/openv/volmgr/database y/n (n)? y
Recovering eel:/usr/openv/volmgr/database
```

You can also use the `-dhost` option to restore from a media server to the master (for example, if the master does not have a drive).

Figure 5. Recover Media Server Databases



5. After recovering databases for the master and all media servers, start the following:
   - `bprd` (NetBackup request daemon)
   - `bpdbm` (NetBackup database manager daemon)
   - `ltid` (Media Manager device daemon)
   - `vmd` (Media Manager volume daemon)

   Use the following commands:

   `/usr/openv/netbackup/bin/initbprd`
   `/usr/openv/volmgr/bin/ltid`

   (Note that `initbprd` starts `bpdbm` and `ltid` starts `vmd`.)

Recover DB from Tape or Optical: Media Manager DB Intact

If the NetBackup database backup is on tape or optical disk and the Media Manager database files are intact, you can recover the databases by using a drive configured under Media Manager control as follows:

1. Stop the NetBackup request daemon (bprd) and NetBackup database manager daemon (bpdbm):
   - Stop bprd by using the Terminate Request Daemon command on the bpadm Special Actions menu (or xbpadm File menu).
   - Stop bpdbm by executing:

     /usr/openv/netbackup/bin/bpdbm -terminate

2. Insert the tape with the catalog backup into an appropriate drive.

   If the tape is not in the drive, the Device Monitor shows a mount request when you start the recovery.

3. On the NetBackup server where the drive attaches, execute the bprecover command.

   Example 1

   Assume the drive is attached to the NetBackup server you are recovering and the backup is on an 8 mm tape that has media ID JBL29. To recover the NetBackup part of the databases from image 1 on the tape:

   ```
   bprecover -r 1 -ev JBL29 -d 8mm
   Recovering shark:/usr/openv/netbackup/db
   ```

   Example 2

   If the drive attaches to another NetBackup server, execute bprecover on the server where the drive attaches and specify the destination server with the -dhost option.

   ```
   bprecover -r 1 -ev JBL29 -d 8mm -dhost shark
   Recovering shark:/usr/openv/netbackup/db
   ```

4. Start the NetBackup request daemon (bprd) and NetBackup database manager daemon (bpdbm) by executing.

   /usr/openv/netbackup/bin/initbprd

   (Note that bprd starts bpdbm)

5. Stop and restart both the device and volume daemons so they can read the recovered configuration.

   a. Stop ltid with the following command:

      /usr/openv/volmgr/bin/stopltid

   b. Stop vmd by executing **/usr/openv/volmgr/bin/vmctrldbm -t** (or use Terminate Media Manager volume Daemon command on the xvmadm File menu).

c. Restart `ltid` by executing:

`/usr/openv/volmgr/bin/ltid`

This automatically starts `vmd`.

Restore DB From Disk

If you backed up the NetBackup databases to a disk that is intact, you can recover the databases as explained in the following procedure.

Note If this disk has failed, you must resort to backups of this disk that have gone to another server. If you have not backed up the NetBackup databases to another server, you must use the NetBackup Import Images feature to import the image information into the databases. See the *NetBackup System Administrator's Guide - UNIX* for instructions.

1. Stop the NetBackup request daemon (`bprd`) and NetBackup database manager daemon (`bpdbm`):

- Stop `bprd` by using the Terminate Request Daemon command on the `bpadm` Special Actions menu (or `xbpadm` File menu).
- Stop `bpdbm` by executing:

  `/usr/openv/netbackup/bin/bpdbm -terminate`

2. Stop the Media Manager device daemon (`ltid`) and Media Manager volume daemon (`vmd`).

- Stop `ltid` by executing:

  `/usr/openv/volmgr/bin/stopltid`

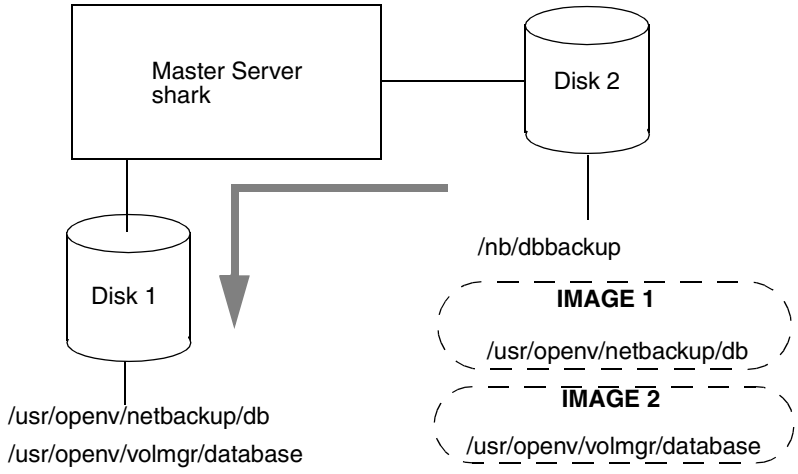
d. Stop `vmd` by executing **`/usr/openv/volmgr/bin/vmctrldbm -t`** (or use Terminate Media Manager volume Daemon command on the `xvmadm` File menu).

3. Execute the `bprecover` command to recover the databases.

The following commands recover the `/usr/openv/netbackup/db` catalogs from disk path `/nb/dbbackup` on Figure 6.

```
bprecover -r 1 -dpath /nb/dbbackup
Recovering shark:/usr/openv/netbackup/db
```

Figure 6. Restore Databases From Disk



4. After recovering the databases, start the following:

- `bprd` (NetBackup request daemon)
- `bpdbm` (NetBackup database manager daemon)
- `ltid` (Media Manager device daemon)
- `vmd` (Media Manager volume daemon)

Use the following commands:

```
/usr/openv/netbackup/bin/initbprd
/usr/openv/volmgr/bin/ltid
```

(Note that `initbprd` starts `bpdbm` and `ltid` starts `vmd`.)

Functional Overview A

This appendix provides a functional overview of NetBackup for both UNIX and Windows NT/2000. Such comprehensive treatment is valuable for mixed-platform environments.

The discussions include descriptions of important daemons and programs, and the sequence in which they execute during typical operations. The databases and the directory structure of the installed software are also described.

There are two main sections in this appendix:

- Backup and Restore Functional Description
- Media Manager Functional Description

It is assumed that you are already familiar with the overviews in the first chapter of the *NetBackup System Administrator's Guide - UNIX* and the *Media Manager System Administrator's Guide - UNIX*.

Note that this appendix does not pertain to the NetBackup products for backing up relational databases (such as NetBackup for ORACLE). The installation guides for those products have information regarding their operation.

Backup and Restore Functional Description

This section explains the operation of NetBackup during backup and restores and contains the following discussions:

- Startup Process
- Backup and Archive Processes
- Restore Processes
- NetBackup Directories and Files
- NetBackup Databases

Startup Process

Before NetBackup can perform scheduled operations or respond to user-directed requests, the NetBackup request daemon `bprd` must be started on the master server, and the Media Manager device daemon `ltid` must be started on the master server and all media servers. These two daemons, in turn, automatically start other daemons and programs as necessary (see Figure 7).

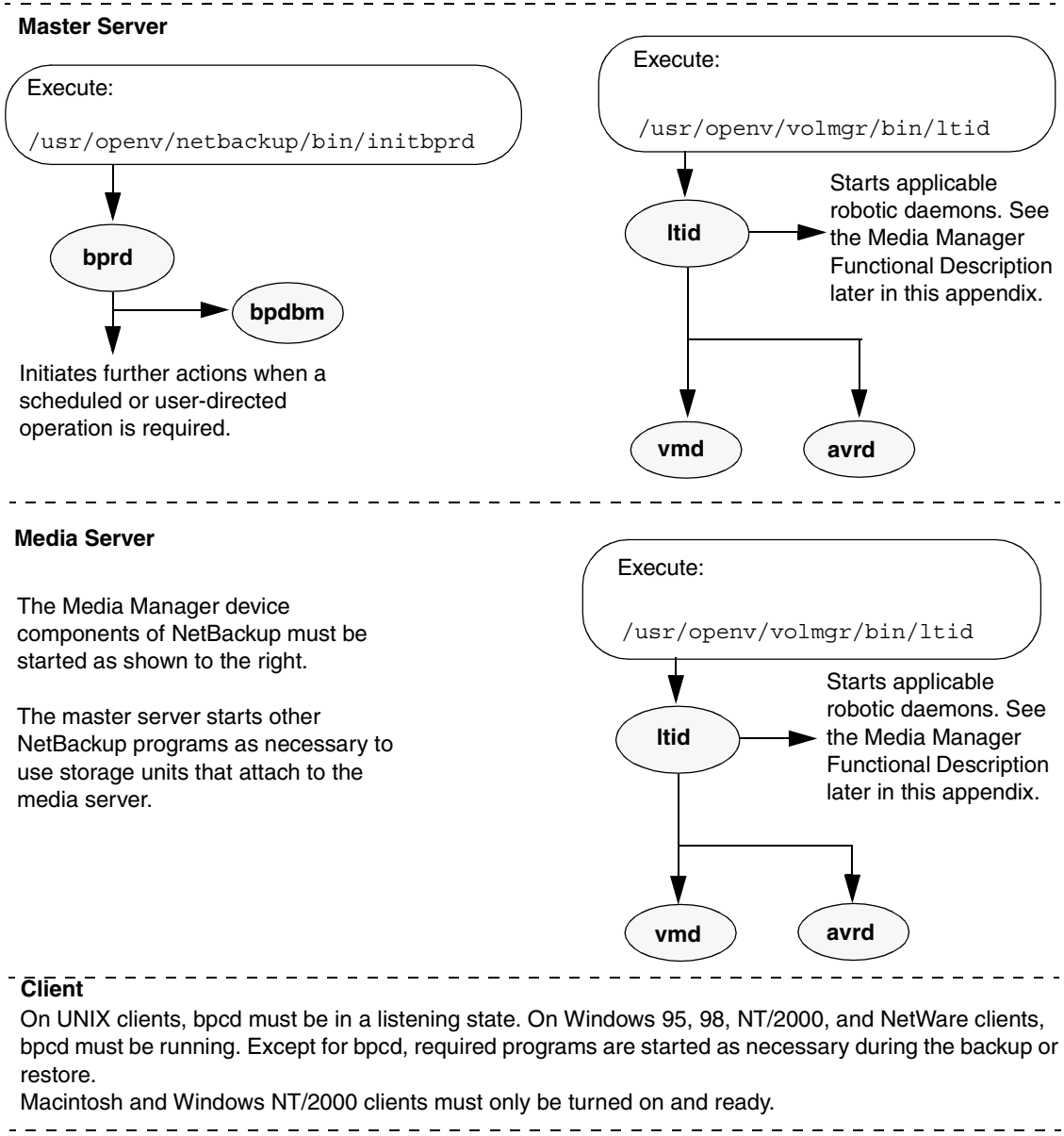
On a media server, it is not necessary to start `bprd` because it is not used. NetBackup automatically starts other required NetBackup programs when it accesses the media server.

Another daemon that executes on all server and clients is the NetBackup client daemon, `bpcd`. On UNIX clients, `inetd` starts `bpcd` automatically so no special actions are required. On Windows NT clients, `bpinetd` performs the same functions as `inetd`. Other PC clients do not use `inetd` or `bpinetd` but are usually configured to start `bpcd` automatically (see their user's guides for instructions).

There are no other daemons or programs that you must explicitly start. The necessary programs are started automatically during the backup or restore operation.

Figure 7 shows the programs that must be running and how they are started. The Media Manager functional description, later in this appendix, has details on the actions started by `ltid`.

Figure 7. Starting NetBackup


Master Server
Execute:
/usr/openv/netbackup/bin/initbprd
bprd
bpdbm
Initiates further actions when a scheduled or user-directed operation is required.
Execute:
/usr/openv/volmgr/bin/ltid
ltid
Starts applicable robotic daemons. See the Media Manager Functional Description later in this appendix.
vmd
avrd
Media Server
The Media Manager device components of NetBackup must be started as shown to the right.
The master server starts other NetBackup programs as necessary to use storage units that attach to the media server.
Execute:
/usr/openv/volmgr/bin/ltid
ltid
Starts applicable robotic daemons. See the Media Manager Functional Description later in this appendix.
vmd
avrd
Client
On UNIX clients, bpcd must be in a listening state. On Windows 95, 98, NT/2000, and NetWare clients, bpcd must be running. Except for bpcd, required programs are started as necessary during the backup or restore.
Macintosh and Windows NT/2000 clients must only be turned on and ready.

Backup and Archive Processes

The backup and archive processes vary depending on the type of client. The following explains the basic variations. There is also a description of how NetBackup operates when backing up its databases.

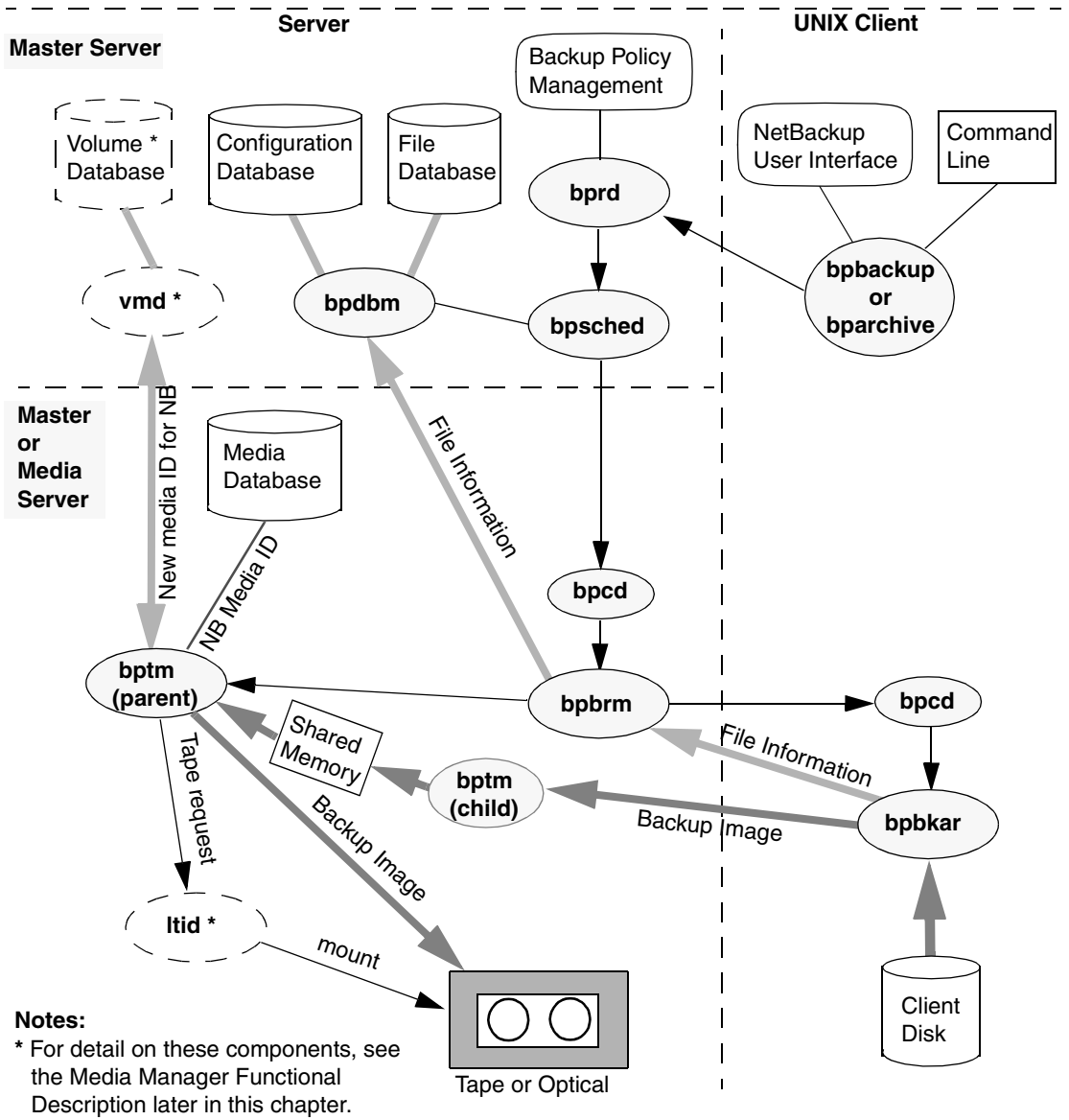
Backups and Archives - UNIX Clients

For UNIX clients, NetBackup supports scheduled, immediate manual, and user-directed backups of both files and raw partitions. User-directed archives of files is also supported (you cannot archive raw partitions). Once started, these operations are all similar to the extent that the same daemons and programs execute on the server (see Figure 8). Each type, however, is started differently.

- Scheduled backup operations begin when the NetBackup request daemon, `bprd`, activates the scheduler, `bpsched`. This occurs at intervals determined by the `Wakeup Interval` global attribute. Once activated, the scheduler checks the class configurations for scheduled client backups that are due.
- Immediate manual backups begin if the administrator chooses the manual backup option in the NetBackup administrator interface. This causes `bprd` to start `bpsched`, which then processes the class, client, and schedule selected by the administrator.
- User-directed backups or archives begin when a user on a client starts a backup or archive through user interface on the client (or the `bpbackup` or `bparchive` commands). This invokes the client's `bpbackup` or `bparchive` program, which sends a request to the request daemon `bprd` on the master server. When `bprd` receives the user request, it starts `bpsched`, which checks the class configurations for schedules and by default chooses the first user-directed schedule that it finds in a class that includes the requesting client. It is also possible to specify a class and schedule by using the NetBackup configuration options, `BPBACKUP_CLASS` and `BPBACKUP_SCHED`, on the client.

  The `bpbackup` and `bparchive` programs execute with the same permissions as the user. If you can read and write files (delete in the case of an archive), they can too.

Figure 8. Backup or Archive to Tape or Optical



For all three types of backup and archive operations, bpsched uses bpcd (client daemon) to start the backup/restore manager (bpbrm). If the required storage unit attaches to the master server, bpsched starts the backup/restore manager on the master server. If the storage unit connects to a media server, bpsched starts the backup/restore manager on the media server.

The backup/restore manager starts the appropriate Media Manager process (bptm for tape or optical and bpdm for disk) and also starts the actual backup (or archive) by using the client daemon (bpcd) to start the backup and archive program (bpbkar) on the client.

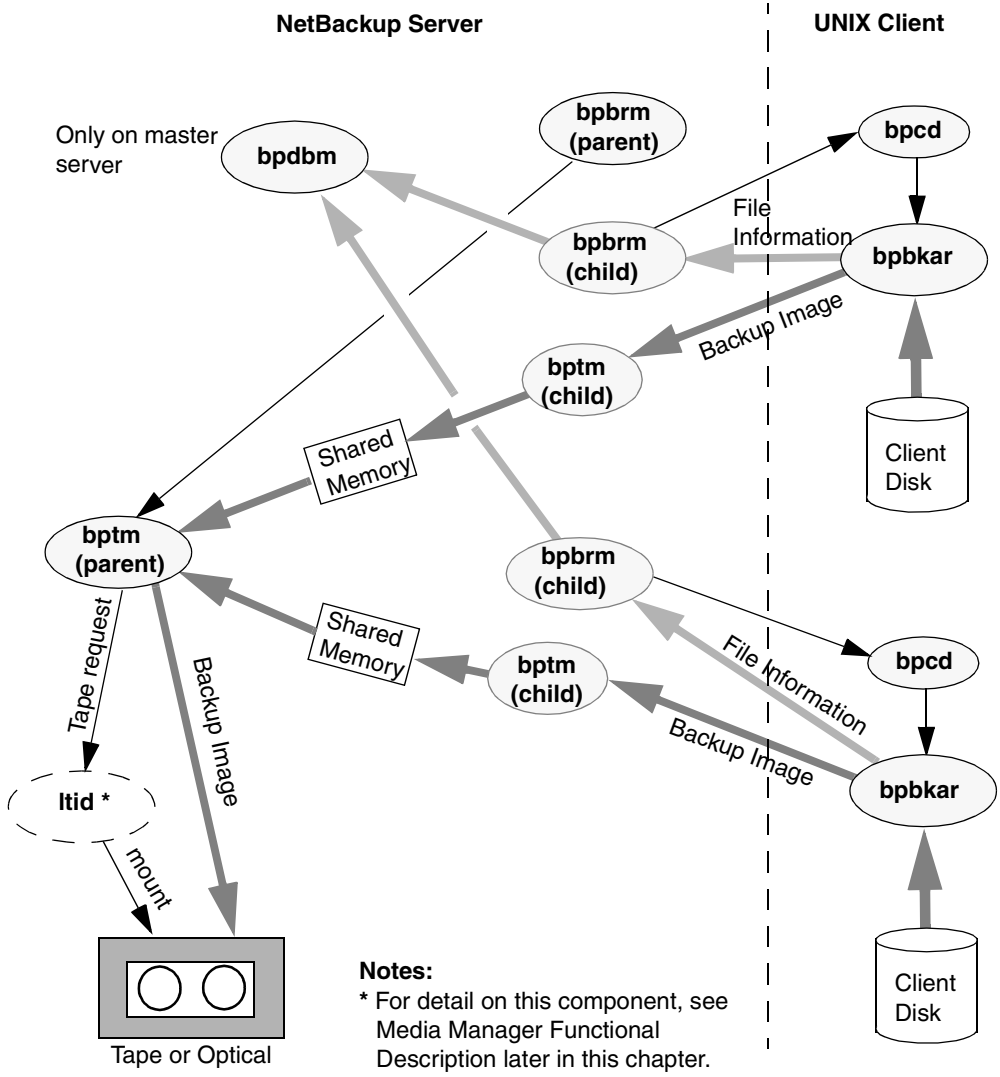
The bpbkar program:

- Sends information about files within the image to the backup/restore manager, which directs the file information to the NetBackup file database.
- Transmits the backup image to the Media Manager process, bptm or bpdm. The bptm or bpdm process forks a second process, which receives the image and stores it block by block in shared memory. The original process then takes the image from shared memory and directs it to the storage media.
  - If the storage is tape or optical, bptm checks the NetBackup media database for a suitable media ID (for example, the correct density and retention level). If it can't find one, it obtains a new media ID from the Media Manager volume daemon, vmd. The bptm program includes the media ID in a tape request to the Media Manager device daemon, ltid, which finds the physical media and causes it to be mounted on an appropriate device. bptm also controls the spanning of backups across multiple tapes, if required.
  - If the storage media is disk, bpdm writes the images to the path configured in the disk storage unit. The system disk manager controls the actual writing of data.

In the case of an archive, NetBackup deletes the files from the client disk after the files have been successfully backed up.

For multiplexed backups, the process is essentially the same except that a separate bpbrm and bptm process is created for each backup image being multiplexed onto the media. NetBackup also allocates a separate set of shared memory blocks for each image. Figure 9 shows an example of multiplexing images from two clients. The other client and server processes are the same as on Figure 8.

Figure 9. Multiplexed Backups Example (two streams)



Backups and Archives - Windows 95/98 Clients

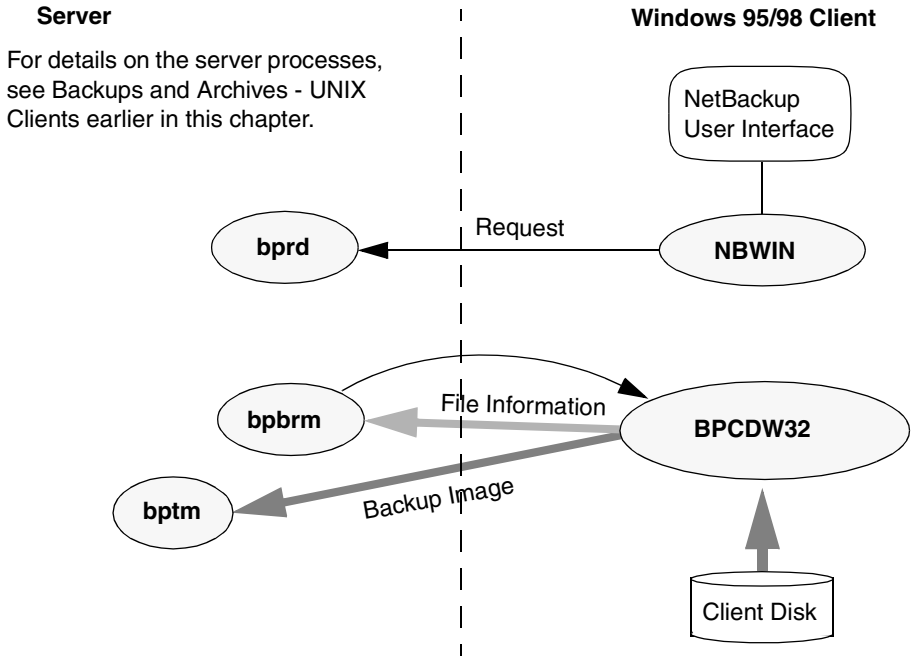
NetBackup supports the same types of operations on Windows 95 and 98 clients as it does for UNIX clients, with the following exception:

- Raw partition backups are not supported.

The next figure shows the Windows 95 and 98 client processes. On this figure:

- The user interface program is called `NBWIN`. The `bpbackup`, `bparchive`, and `bplist` functions are merged into `NBWIN`.
- The NetBackup client daemon is called `BPCDW32`. The `bpbkar` functions are merged into `BPCDW32`.

The server processes are the same as described for UNIX.



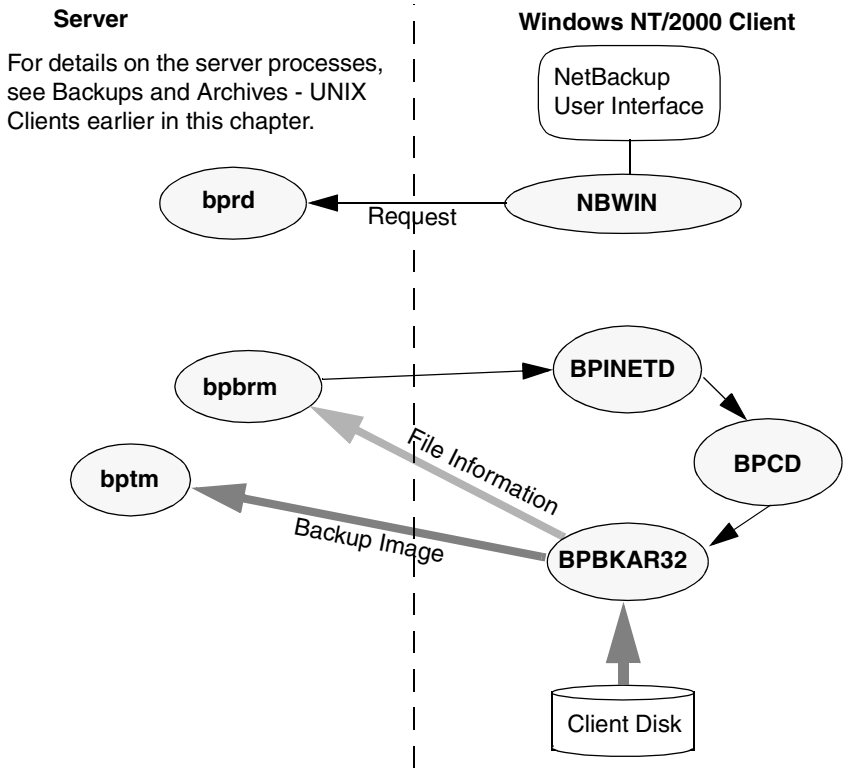
Backups and Archives - Windows NT/2000 Clients

NetBackup supports the same types of operations on Windows NT/2000 clients as it does for UNIX clients.

The next figure shows the Windows NT/2000 client processes. On this figure:

- `NBWIN` is the user interface program on the client. The `bpbackup`, `bparchive`, and `bplist` functions are merged into `NBWIN`.
- `BPINETD` serves the same purpose as `inetd` on UNIX clients.
- The NetBackup client daemon is called `BPCD`.
- `BPBKAR32` serves the same purpose as `bpbkar` on UNIX clients.

The server processes are the same as described for UNIX.



Backups and Archives - NetWare Clients

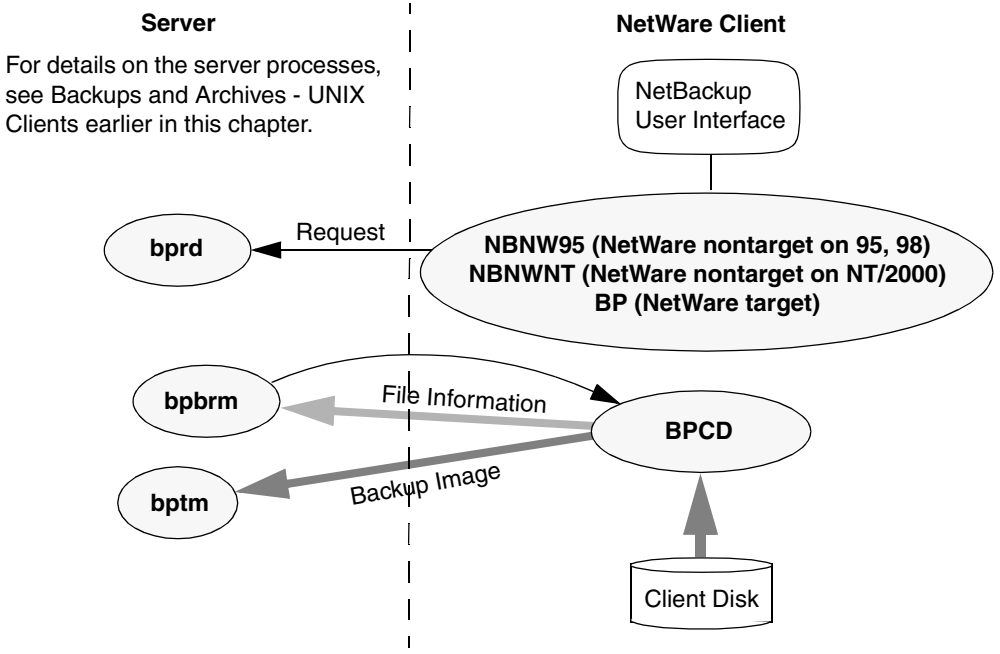
NetBackup supports the same types of operations on NetWare clients as it does on UNIX clients, with the following exceptions:

- Raw partition backups are not supported.
- NetBackup for NetWare does not support archiving.

The next figure shows the NetWare client processes. On this figure:

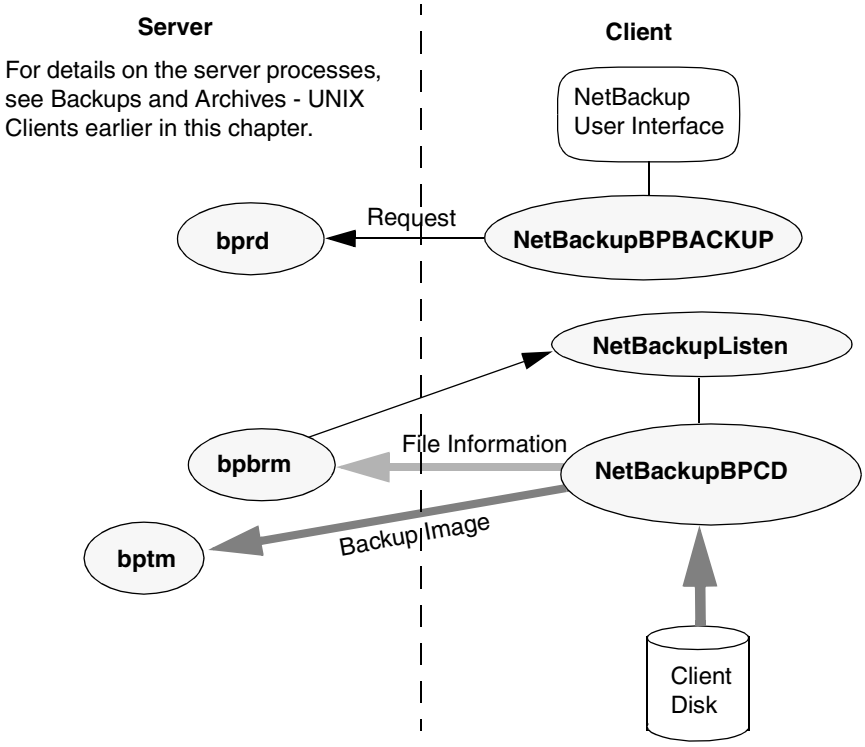
- For NetWare nontarget, the user interface program is called `NBNW95` on Windows 95 and 98 clients and `NBNWNT` on Windows NT/2000. For NetWare target, the user interface program is called `BP` on the Netware console. The `bpbackup`, `bparchive`, and `bplist` functions are merged into the user interface programs on the clients.
- The NetBackup NetWare client daemon is called `BPCD`. The `bpbkar` functions are merged into `BPCD`.

The server processes are the same as described for UNIX.



Backups - Macintosh Clients

NetBackup supports the same types of operations on Macintosh clients as it does for UNIX clients. The next figure shows the client processes involved in backing up a Macintosh. The server processes are the same as described for UNIX.



- `NetBackupBPBACKUP` is a faceless background application that NetBackup launches in order to start a user-directed backup.
- The application extension, `NetBackupListen`, starts executing when the Macintosh is booted and listens on the `BPCD` port number for backup requests from a NetBackup server. When `NetBackupListen` gets a request, it launches the faceless background application `NetBackupBPCD`.
- `NetBackupBPCD` handles the request in the same way as the UNIX `bpcd`. `NetBackupBPCD` also includes `bpbkar` functionality.

The archive that the Macintosh client generates is essentially the same as the archive from a UNIX client. One difference is that the Macintosh file names may be slightly different in the NetBackup archive (see the *NetBackup User's Guide - Macintosh* for an explanation of the differences).

NetBackup Database Backups

The administrator can use an option in the administrator interface to start a manual backup of the NetBackup databases or configure NetBackup to automatically back up its databases (Figure 10).

It is possible to configure automatic database backups to occur either:

- After each scheduled backup session that results in the creation of at least one backup image.

  Or

- After scheduled, user-directed, or manual backup or archive sessions that result in the creation of at least one backup or archive image.

For automatic database backups, NetBackup uses the scheduler, `bpsched`, to determine if any backups are required. The scheduler is activated by the request daemon, `bprd`, at intervals determined by the `Wakeup Interval` global attribute. If a backup is needed, `bpsched` uses the client daemon, `bpcd`, to start the database backup program, `bpbackupdb`.

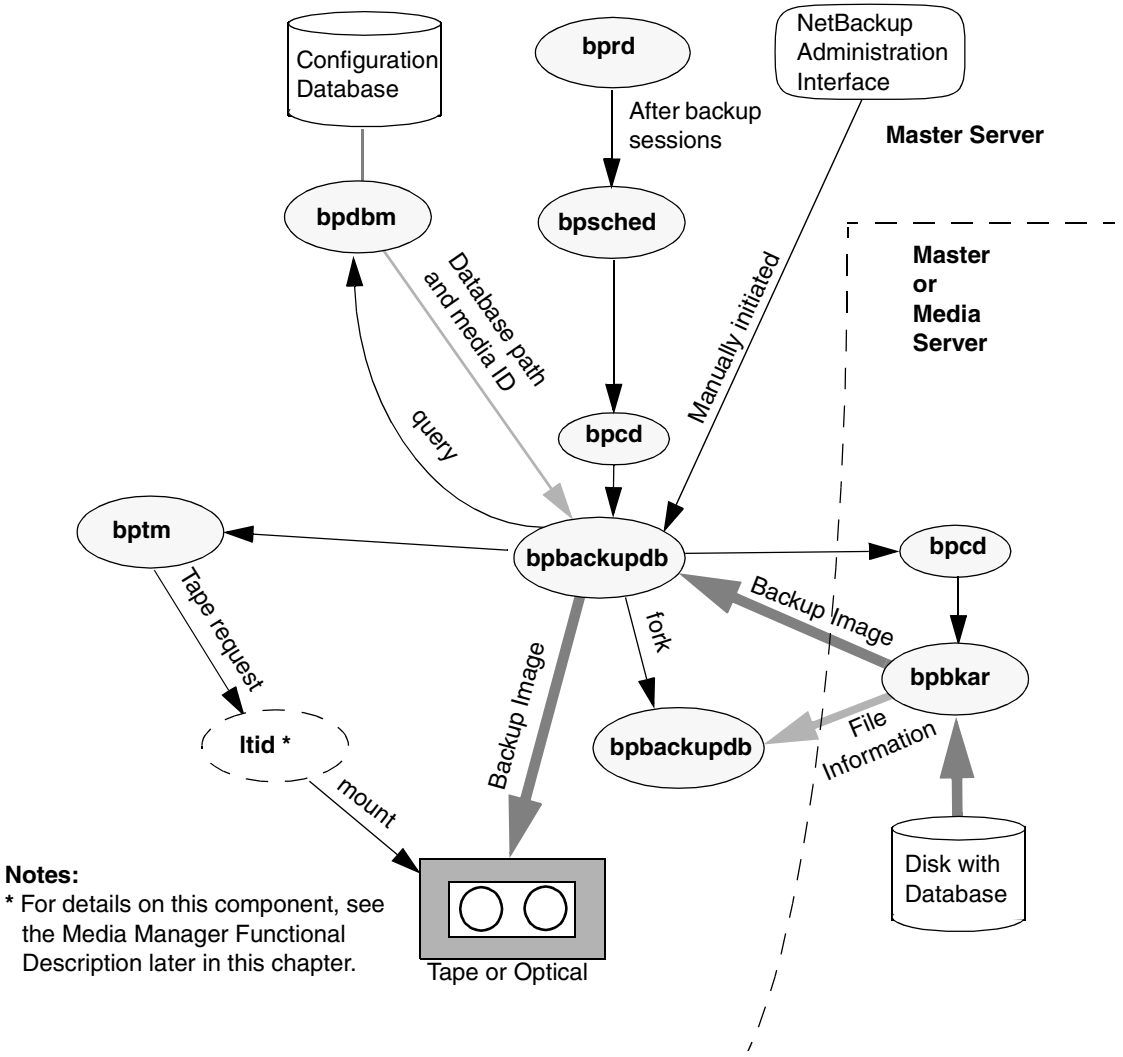
For a manual database backup, NetBackup invokes `bpbackupdb` directly, without going through `bprd` or the scheduler.

Once started, `bpbackupdb`:

1. Queries `bpdbm` for the database paths to back up and the media ID to use for the backup.
2. Starts the tape and optical manager, `bptm`, and sends it the media ID in a special mount request.

   The tape and optical manager, `bptm`, recognizes the request as being for a database backup and checks the database to ensure that the media ID is not one used for regular backups. The `bptm` program then includes the media ID in a request to the Media Manager device daemon, `ltid`. The device daemon finds the media and causes it to be mounted on an appropriate device.

Figure 10. NetBackup Database Backup



3. Starts the actual backup by using `bpcd` to start the backup program, `bpbkar`.

If the database is on the master server, `bpbackupdb` starts the backup and archive program on the master server. If the database is on a media server, `bpbackupdb` starts the backup and archive program on the media server.

The `bpbkar` program transmits file information and the backup image to separate `bpbackupdb` processes as shown on Figure 10.

- The original `bpbackupdb` process receives the backup image and sends it to the backup device.

- A second bpbackupdb process checks the file information to ensure that the proper files are being backed up.

The entire database backup must fit on a single tape. The bpbackupdb process is unable to span tapes and there is no mechanism for specifying multiple tapes for an NetBackup database backup.

If any part of the database backup fails, then NetBackup discards the entire backup. This is done because you must have a backup of *all* the databases to be certain that you have a consistent database.

Restore Processes

NetBackup restore operations, like backups, can vary according to client type. The following explains the basic variations.

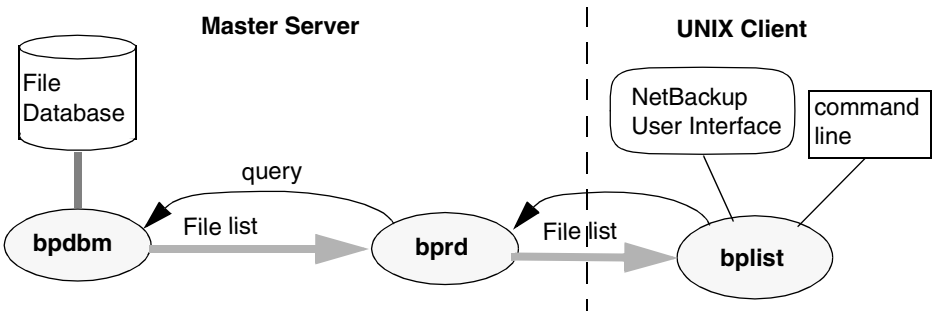
Restores - UNIX Clients

Before starting a restore operation, a user will usually browse the file database and list the files available in the backup images. The desired files can then be selected from the list.

The browsing is done through the bplist program on the client. The bplist program can be started directly from the command line and is used by the NetBackup user interface programs.

bplist obtains the file list by sending a query to the request daemon, bprd, on the master server (Figure 11). The request daemon, in turn, queries bpdbm for the information and transmits it to bplist on the client.

Figure 11. List Operation - UNIX Client



When the user starts a restore, NetBackup invokes the client's bprestore program which sends a request to the request daemon, bprd (Figure 12). This request identifies the files and client. The request daemon then uses bpcd (client daemon) to start the backup/restore manager (bpbrm).

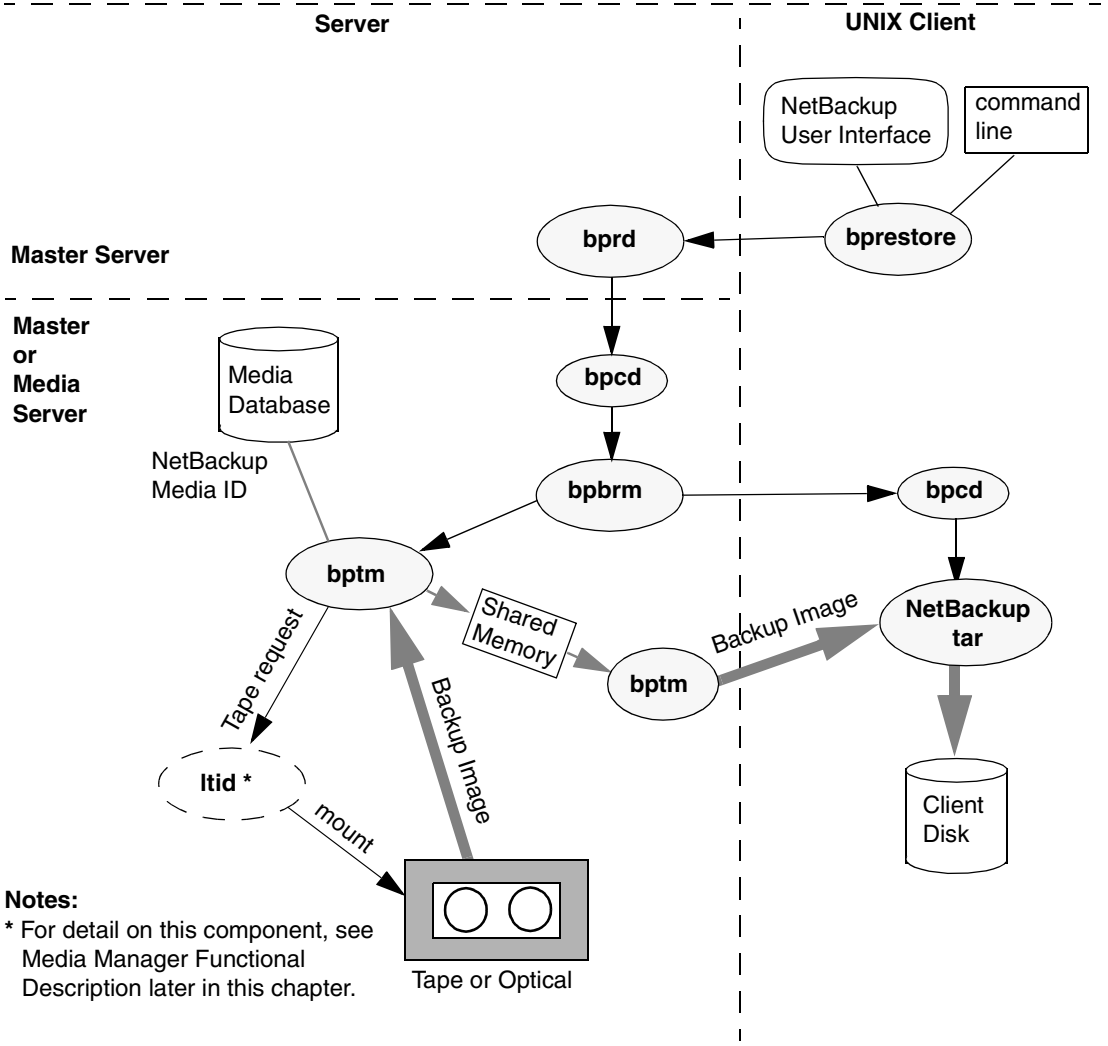
If the storage unit on which the files reside attaches to the master server, then bprd starts the backup/restore manager on the master server. If the storage unit connects to a media server, bprd starts the backup/restore manager on the media server.

The backup/restore manager starts the appropriate Media Manager process (bptm for tape or optical or bpdm for disk) and uses the client daemon (bpcd) to establish a connection between the NetBackup tar program on the client and bptm or bpdm on the server.

The bptm (for tape or optical) or bpdm (for disk) process obtains the location of the data (media ID or file path) and then starts retrieving data. During retrieval, the original bptm or bpdm process stores the image block by block in shared memory. A second bptm or bpdm process transmits the image to the client.

- If the storage is tape or optical, bptm includes the media ID in a tpreq command to the Media Manager device daemon, ltid. The device daemon finds the physical media and causes it to be mounted on an appropriate device. The bptm program reads the image and directs it to the client, where the NetBackup tar program writes it on the client disk.
- If the storage unit is disk, bpdm uses the file path in a read request to the system disk manager. The image is then read from disk and transmitted to the client, where the NetBackup tar program writes it on the client disk. Only the part of the image that is required to satisfy the restore request is sent to the client, not necessarily the entire backup image.

Figure 12. Restore operation From Tape or Optical

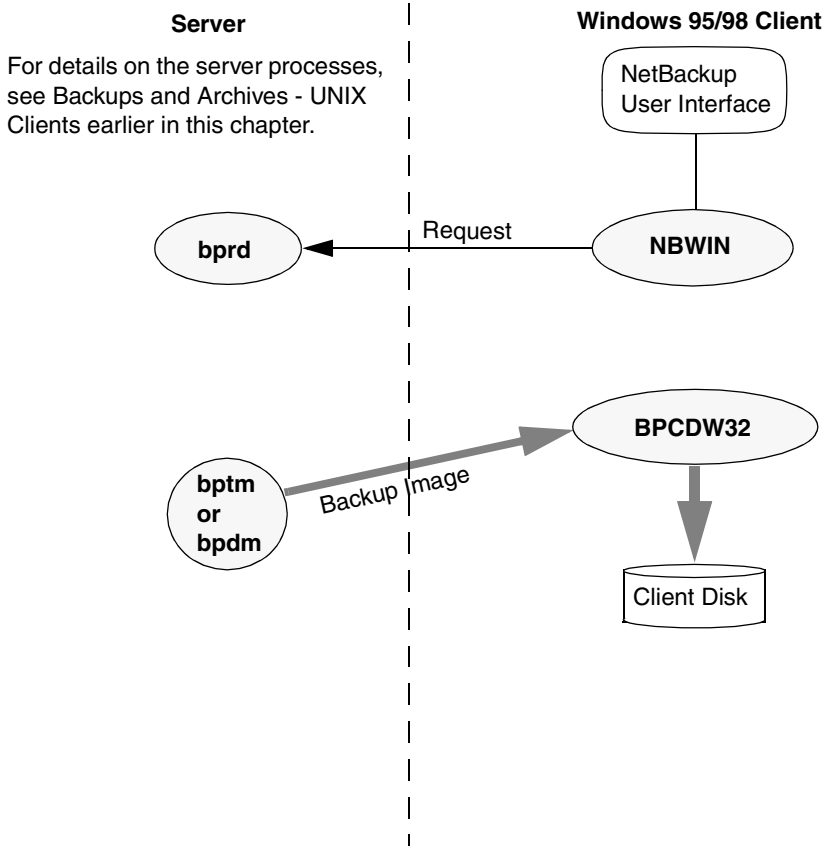


Restores - Windows 95/98 Clients

NetBackup supports the same types of restore operations on Windows 95 and 98 clients as it does for UNIX clients. The next figure shows the client processes involved in these operations. On this figure:

- The user interface program on Windows 95/98 is called `NBWIN`. The `bprestore` and `bplist` functions are merged into `NBWIN`.
- The NetBackup client daemon is called `BPCDW32`. The NetBackup `tar` functions are merged into `BPCDW32`.

The server processes are the same as described for UNIX.

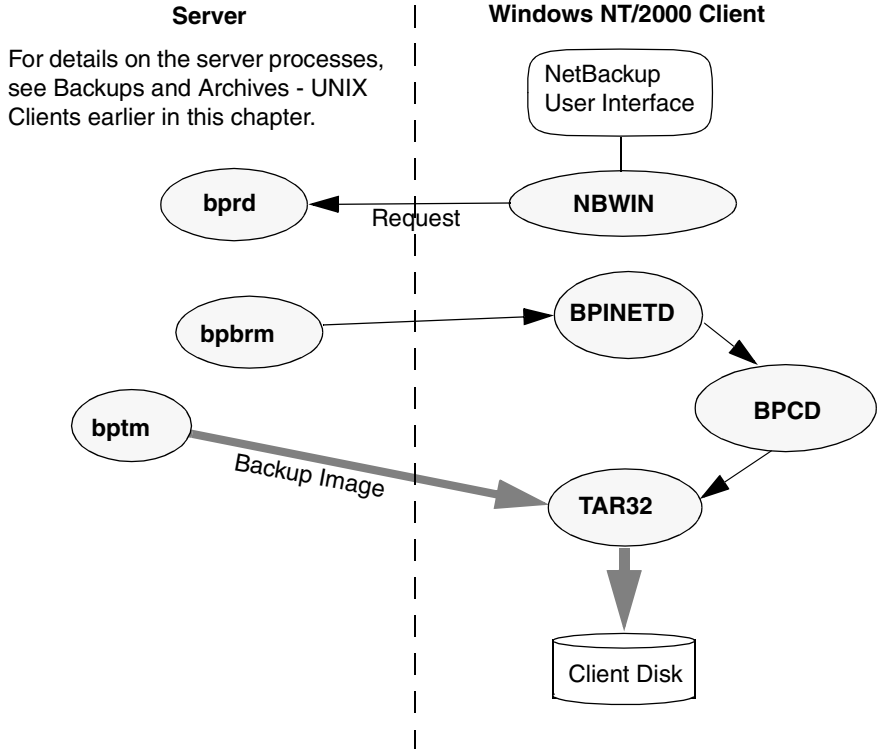


Restores - Windows NT/2000 Clients

NetBackup supports the same types of operations on Windows NT/2000 clients as it does for UNIX clients. The next figure shows the client processes involved in these operations.

- The user interface program on Windows NT/2000 is called `NBWIN`.
- `BPINETD` is part of NetBackup for Windows NT/2000 and serves the same purpose as `inetd` on UNIX.
- The NetBackup client daemon is called `BPCD`.
- `TAR32` is part of NetBackup for Windows NT/2000 and serves the same purpose as NetBackup `tar` on UNIX.

The server processes are the same as described for UNIX.

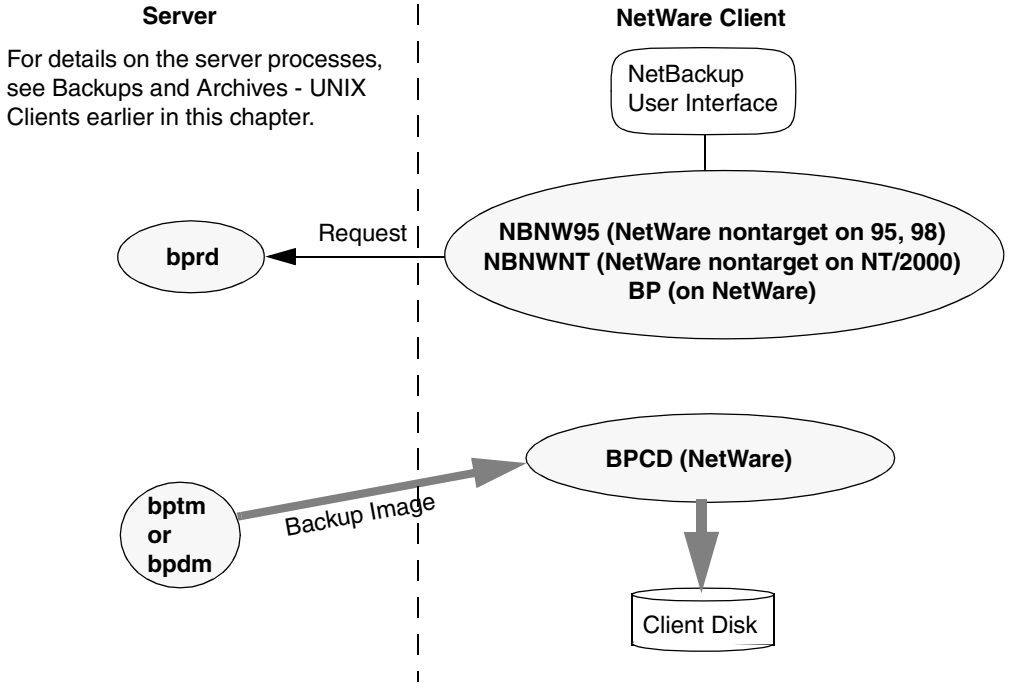


Restores - NetWare Clients

NetBackup supports the same types of restore operations on NetWare clients as it does on UNIX clients. The next figure shows the client processes involved in these operations. On this figure:

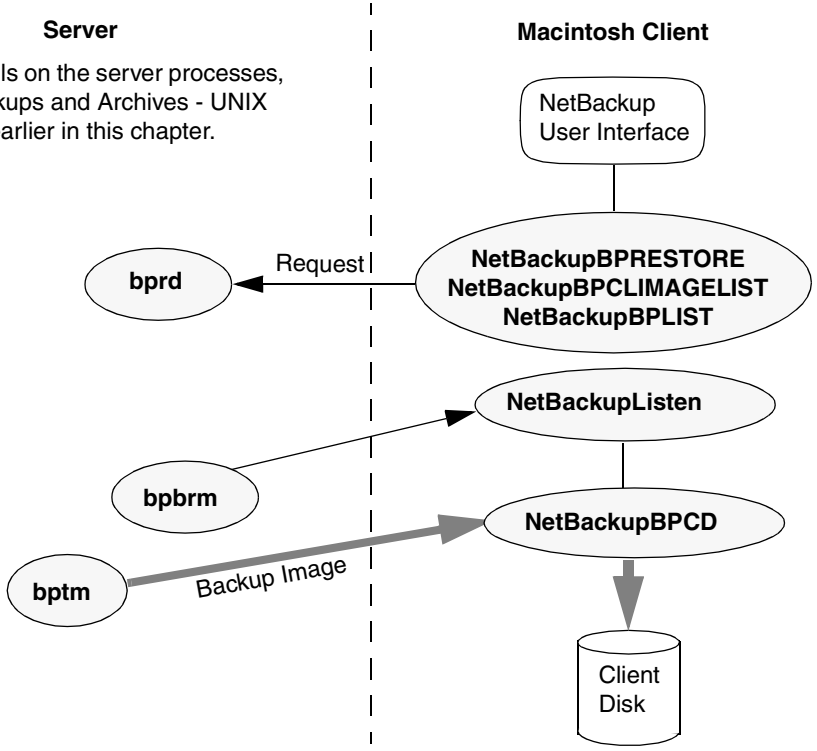
- The NetWare nontarget user interface program is called `NBNW95` on Windows 95 and 98 clients and `NBNWNT` on Windows NT/2000 clients. The NetWare target user interface program is `BP` on the Netware console. The `bprestore` and `bplist` functions are merged into the user interface programs on the clients.
- The NetBackup NetWare client daemon is called `BPCD`. The NetBackup `tar` functions are merged into `BPCD`.

The server processes are the same as described for UNIX.



Restores - Macintosh Clients

NetBackup supports the same types of operations on Macintosh clients as it does for UNIX clients. The next figure shows the client processes involved in restoring files to a Macintosh.



- `NetBackupBPRESTORE` is a faceless background application that NetBackup launches in order to start a user-directed restore.
- `NetBackupCLIMAGELIST` is a faceless background application that NetBackup launches in order to get a list of backup images from the master server.
- `NetBackupBPLIST` is a faceless background application that NetBackup launches in order to get a list of backed up files from the master server.
- The application extension `NetBackupListen` starts executing when the Macintosh is booted and listens on the `BPCD` port number for backup requests from a NetBackup server. When `NetBackupListen` gets a request, it launches the faceless background application `NetBackupBPCD`.
- `NetBackupBPCD` handles the request in the same way as the UNIX `bpcd`. `NetBackupBPCD` also includes NetBackup `tar` functionality.

The server processes are the same as described for UNIX.

NetBackup Directories and Files

Figure 13 shows the NetBackup file and directory structure on UNIX servers and clients. If a host is only a client and not a server, then only the files in the lower part of Figure 13 are present. If a host is both a client and a server, the client component shares files as necessary from those in the upper part of Figure 13.

A Windows NT/2000 NetBackup server has equivalent files and directories that are located in the directory where NetBackup is installed (`c:\Veritas` by default).

Table 6 describes the files and directories that are of special interest.

Figure 13. NetBackup Directories and Files - UNIX Servers and Clients

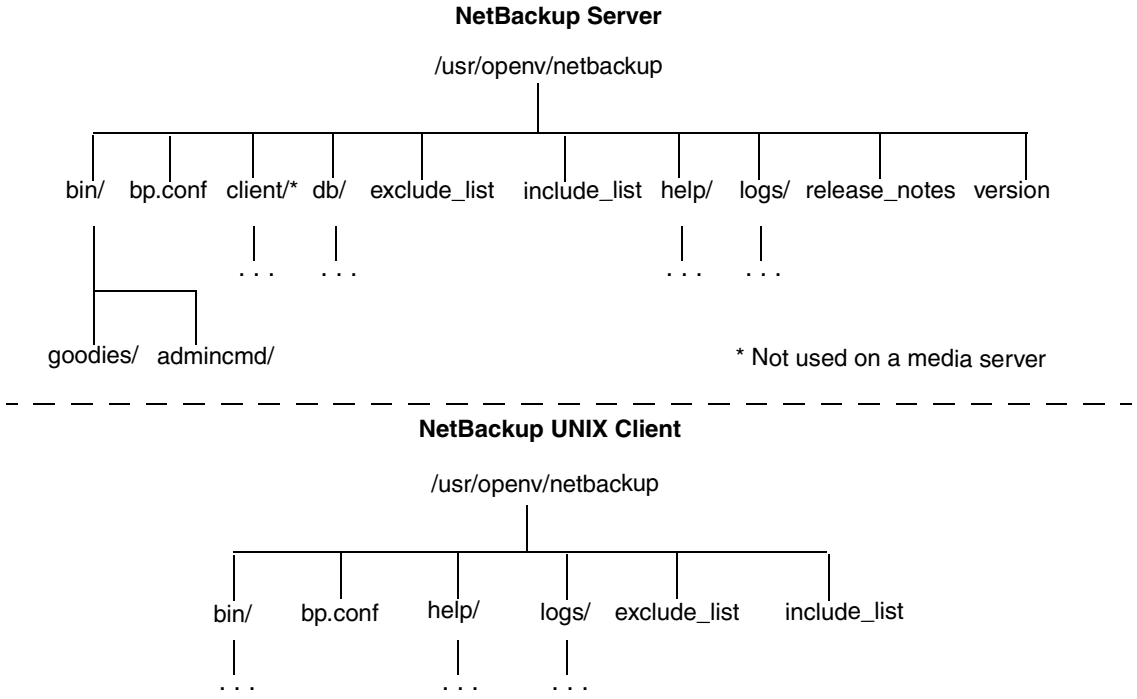


Table 6. NetBackup Directories and Files - Servers and UNIX Clients

File or Directory	Contents
`bin`	Commands, scripts, programs, daemons, and files required for NetBackup operation and administration. On a server, there are two subdirectories under bin. admincmd: Contains various commands used internally by NetBackup. Use these commands *ONLY* if they are documented. Most of these commands are not documented and should not be used directly. `goodies` (UNIX only): Contains scripts and information that may be useful to the administrator. These subdirectories are not present on clients.
`bp.conf`	Configuration file where you can specify various options for NetBackup operation. The *NetBackup System Administrator's Guide* has a detailed explanation of each option and how to set it. On a Windows NT/2000 server, these options are set in the interface.
`client`	NetBackup client software that is installed on the clients during the installation process. Do not install this directory on a media server.
`db`	NetBackup databases as described in Table 8.
`exclude_list`	On UNIX clients, this file contains a list of files and directories to exclude from scheduled backups. The *NetBackup System Administrator's Guide* explains how to use this file.
`help`	Help files used by NetBackup programs. These files are in ASCII format.
`include_list`	On UNIX clients, this file contains a list where you can specify a subset of the exclude list to add back into scheduled backups. The *NetBackup System Administrator's Guide* explains how to use this file.
`logs`	Detailed activity logs for NetBackup processes. You must create the necessary subdirectories for these logs to be created (see Chapter 3). See Table 7 for an explanation of the processes that produce the logs.
`release_notes`	NetBackup release notes in ASCII format, so you can conveniently view or print them.
`version`	Version and release date of the software.

NetBackup Programs and Daemons

Table 7 describes the programs and daemons that provide most of the control for backup, archive, and restore operations. The explanations include what starts and stops the program or daemon, and the log (if any) where it records its activities.

Table 7. NetBackup Daemons and Programs

Program/ Daemon	Description
bp	On UNIX clients, this menu-driven, character-based interface program has options for starting user-directed backups, restores, and archives. **Started By:** /usr/openv/netbackup/bin/bp command on the client. **Stopped By:** Exiting the interface program. **Activity Log:** /usr/openv/netbackup/logs/bp on the client. The activity logs for bpbackup, bparchive, bprestore, and bplist also have information about bp activities.
BP.NLM	On NetWare target clients, this is the NetWare Loadable Module that starts the client-user interface. **Started By:** LOAD BP command. **Stopped By:** Choosing Quit Utility from the main menu. **Activity Log:** SYS:\OPENV\NETBACK\LOGS\BP*mmddyy*.log file on the client.
bpadm	On a UNIX master server, this administrator utility has a menu-driven, character-based, interface with options for configuring and managing NetBackup. **Started By:** /usr/openv/netbackup/bin/bpadm command on the master server. **Stopped By:** Quit option from within bpadm. **Activity Log:** admin.log on the server.
bparchive	On UNIX clients, this program communicates with bprd on the master server when a user starts an archive. **Started By:** Starting an archive by using the client-user interface or executing the /usr/openv/netbackup/bin/bparchive command on the client. **Stopped By:** Completion of operation. **Activity Log:** bparchive.log on the client.

Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
bpbackup	On UNIX clients, this program communicates with bprd on the master server when a user starts a backup. **Started By:** Starting a backup by using the client-user interface or executing the /usr/openv/netbackup/bin/bpbackup command on the client. **Stopped By:** Completion of operation **Activity Log:** bpbackup.log on the client.
bpbrm	On master and media servers, the Backup/Restore Manager manages the client and Media Manager processes and uses error status from both to determine the final status of backup or restore operations. **Started By:** For each backup or restore, bpsched starts an instance of bpbrm on the server with the appropriate storage unit. **Stopped By**: Completion of operation. **Activity Log:** bpbrm.log on the server.
bpbkar	On UNIX clients (except Apollos), the Backup/Archive Manager generates the backup images. **Started By:** bpbrm on the server with the storage unit. **Stopped By:** Completion of operation. **Activity Log:** bpbkar.log on the client.
BPBKAR32	On Windows NT/2000 clients, the Backup/Archive Manager generates the backup images. **Started By:** BPCDW32 on the client. **Stopped By:** Completion of operation. **Activity Log:** BPBKAR.LOG file in the NetBackup logs directory on the client.

Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
bpcd	On UNIX clients, bpcd is the NetBackup client daemon and lets NetBackup start programs on remote hosts (can be UNIX clients or other servers). For example, the server can connect to UNIX clients without requiring /.rhosts entries on the remote host. The program is used when bpsched starts bpbrm and when bpbrm communicates with the client. (For a description of the NetBackup client daemon on PC clients, see BPCDW32.EXE, BPCD.NLM, and NetBackupBPCD later in this table.) **Started By:** inetd. **Stopped By:** Completion of operation. **Activity Log:** bpcd.log on both client and server.
BPCD.NLM	On NetWare clients, this is the executable file that starts the NetBackup client daemon. **Started By:** When you start the Novell NetWare system if you add load bpcd to the AUTOEXEC.NCF file. Otherwise, with the LOAD BPCD command. **Stopped By:** UNLOAD BP command **Activity Log:** BPCD.LOG file in the NetBackup logs directory on the client.
BPCDW32.EXE	On Windows 95 and NT/2000 clients, this is the executable file that starts the NetBackup client daemon. **Started By:** When Windows starts if the daemon is in the Startup group. Otherwise, by double clicking on its icon. **Stopped By:** On Windows NT/2000, you can stop it through the Services application in the Control Panel. On Windows 95, you can stop it by clicking on its icon and choosing Close. **Activity Log:** BPCD.LOG file in the NetBackup logs directory on the client.
bpdbjobs	On UNIX master servers, this program is used to clean up the NetBackup jobs database. **Started By:** /usr/openv/netbackup/bin/admincmd/bpdbjobs. When bprd starts, it runs this command automatically. The administrator can also execute it manually or with a cron job. **Stopped By:** There is no terminate option for this command outside of using kill. **Activity Log**: bpdbjobs.log on the server.

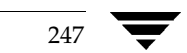


Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
bpdbm	On master servers, the NetBackup program that manages the configuration, error, and file databases. **Started By:** bprd (also by /usr/openv/netbackup/bin/initbpdbm on UNIX) **Stopped By:** /usr/openv/netbackup/bin/bpdbm -terminate command on UNIX and by stopping the NetBackup Database Manager service on Windows NT/2000. **Activity Log:** bpdbm.log on the server.
bpdm	On master and media servers, bpdm is the disk-media manager and is used when the storage unit type is a disk. This program manages the transfer of images between the client and the operating-system disk manager on the server to which the disk attaches. **Started By:** For each backup or restore, bpbrm starts an instance of bpdm, on the server with the storage unit. **Stopped By:** Completion of operation. **Activity Log:** bpdm.log on the server.
bphdb	On UNIX database-extension clients, bphdb starts the NetBackup hot-database-backup program (see the applicable NetBackup installation guide for more information). **Started By:** Client-user interface when the user starts a database backup or restore operation. **Stopped By:** Completion of operation. **Activity Log:** bphdb.log on the client. With NetBackup for Oracle, bphdb also writes to /usr/openv/netbackup/logs/obackup_tape.
bpjava-msvc	NetBackup-Java master server application program. This program runs on all NetBackup UNIX systems and authenticates users that start the NetBackup-Java interface programs. **Started By:** inetd during startup of the NetBackup Java interfaces. **Stopped By:** When authentication is complete. **Activity Log:** /usr/openv/netbackup/logs/bpjava-msvc

Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
bpjava-usvc	NetBackup-Java user server application program. This program services all requests from the NetBackup-Java user and administration interfaces. **Started By:** bpjava-msvc upon successful login through the Login dialog box that is presented when a NetBackup-Java interface is started. **Stopped By:** When the interface program is terminated. **Activity Log:** /usr/openv/netbackup/logs/bpjava-usvc
bprd	On master servers, the request daemon responds to client and administrative requests for the following: ◆ Restores ◆ Backups (scheduled and user-directed) ◆ Archives ◆ List backed up or archived files ◆ Manual immediate backups (started through the NetBackup administration interface manual backup option) **Started By:** Initiate Request Daemon option in the NetBackup administrator interface (also the /usr/openv/netbackup/bin/initbprd command). **Stopped By:** Terminate Request Daemon option in the NetBackup administrator interface. **Activity Log:** bprd.log on the server.
bplist	On UNIX clients, this program communicates with bprd on the master server when a user browses the database during a restore operation. **Started By:** Starting a search of the image database by using the client-user interface or executing the /usr/openv/netbackup/bin/bplist command on the client. **Stopped By:** Completion of operation **Activity Log:** bplist.log on the client.
bprestore	On UNIX clients, this program communicates with bprd on the master server when a user starts a restore. **Started By:** Starting restore by using the client-user interface (or by executing the /usr/openv/netbackup/bin/bprestore command on the client). **Stopped By:** Completion of operation **Activity Log:** bprestore.log on the client.

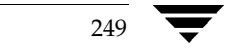


Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
bpsched	On master servers, the Scheduler uses class information from the NetBackup configuration databases to determine: ◆ Clients to start and when to start them. ◆ Storage units to use for backups and archives. **Started By:** bprd for the following operations: ◆ User-directed backups and archives ◆ Immediate manual backups (started through the option that is available in the NetBackup administrator interface) ◆ Scheduled automatic incremental or full backups. In this case, bprd starts the scheduler at intervals determined by the wakeup interval global attribute. **Stopped By:** Completion of all backups that are due. **Activity Log:** bpsched.log on the server.
bptm	On master and media servers, bptm is the tape-media manager and is used when the storage unit type is Media Manager. This program manages transfer of images between the client and the storage device. It also handles communication between the backup and Media Manager software. In addition, bptm manages the NetBackup media database and provides information for the media list report screen. **Started By:** For each backup or restore, bpbrm starts an instance of bptm on the server that has the storage unit. **Stopped By:** Completion of operation. **Activity Log:** bptm.log on the server.
BPSRV.EXE	On NetWare nontarget clients, this is the program that allows the system that has the client-user interface to communicate with the Netware server that is the NetBackup client. **Started By:** Starting NetBackup for NetWare. **Stopped By:** Exiting the client-user interface. **Activity Log:** BPSRV.LOG file in the NetBackup LOGS directory on the client.
BPSYS.EXE	On Windows NT/2000 clients, this is the NetBackup System Registry Replacement utility. **Started By:** NetBackup as required. **Stopped By:** Completion of operation. **Activity Log:** BPSYS.LOG file in the NetBackup LOGS directory on the client.

Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
jbpSA	A Java-based program for performing backups, archives and restores of UNIX clients. **Started By:** On UNIX, the /usr/openv/netbackup/bin/jbpSA command. **Activity Log:** None, although the log for the bpbackup, bparchive, bplist, and bprestore commands on the client can be useful. Also, the logs for bpjava-msvc and bpjava-usvc can be helpful.
jnbSA	A Java-based administration utility for managing NetBackup and Media Manager on UNIX. In addition, administration of supported UNIX systems can be performed by using the NetBackup-Java Windows Display Console on a Windows NT/2000 system. **Started By:** On UNIX, the /usr/openv/netbackup/bin/jnbSA command. On a NetBackup-Java Windows Display console, the NetBackup - Java on *host* menu item on the Programs/NetBackup menu. **Stopped By:** Exit option in jnbSA. **Activity Log:** None, although the logs for bpjava-msvc and bpjava-usvc can be helpful.
NBWIN.EXE	For Windows clients, this is the executable file that starts the client-user interface on Windows NT/2000, 98 and 95 systems. **Started By:** From the Windows Start menu, under Programs/ NetBackup. **Stopped By:** Exiting the client-user interface. **Activity Log:** *mmddyy*.log file in the NBWIN directory on the client.
NBNWNT.EXE	For NetWare nontarget clients, this is the executable file that starts the client-user interface on Windows NT/2000 systems. **Started By:** From the Windows Start menu, under Programs/ NetBackup. **Stopped By:** Exiting the client-user interface. **Activity Log:** none.

Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
NBNW95.EXE	For NetWare nontarget clients, this is the executable file that starts the client-user interface on Windows 98/95 systems. **Started By:** From the Windows Start menu, under Programs/ NetBackup. **Stopped By:** Exiting the client-user interface. **Activity Log:** none.
NetBackupBPCD	A faceless background application installed in the System:Extensions folder on the startup volume of a Macintosh client. The Macintosh equivalents of the UNIX bpbkar and tar commands are merged into NetBackupBPCD. **Started By:** When NetBackupListen receives a request from a server it launches NetBackupBPCD. **Stopped By:** Completion of operation. **Activity Log:** Log files in the System:Preferences:NetBackup:bpcd folder, which is in the NetBackup folder, in the Preferences folder, in the System folder on the startup volume.
NetBackupListen	An applications extension installed in the System:Extensions folder on the startup volume of a Macintosh client. It starts when the Macintosh is booted and runs in the background until the Macintosh is shut down. NetBackupListen listens on the BPCD port number for requests from NetBackup servers and launches NetBackupBPCD when a request is received. **Started By:** When the Macintosh boots. **Stopped By:** When the Macintosh is shut down. **Activity Log:** Log files in the System:Preferences:NetBackup:inetd folder on the startup volume.
tar	On UNIX clients, the Tape ARchive program is a special version of tar provided with NetBackup and used to restore images. **Started By:** For each restore, bpbrm starts an instance of tar on the client. **Stopped By:** Completion of restore operation. **Activity Log:** tar.log on the client.

Table 7. NetBackup Daemons and Programs (continued)

Program/ Daemon	Description
TAR32	On Windows NT/2000 clients, the TAR32 program is a special version of tar provided with NetBackup and used to restore images. **Started By:** For each restore, NetBackup starts an instance of TAR32 on the client. **Stopped By:** Completion of restore operation. **Activity Log:** TAR.LOG in the NetBackup logs directory on the client.
xbp	X Windows based client-user interface, on UNIX clients, with options for starting user-directed backups, restores, and archives. Functionally, it is very similar to the menu version, bp. **Started By:** /usr/openv/netbackup/bin/xbp command on the client. **Stopped By:** Quit option in xbp. **Activity Log:** None, although the log for the bpbackup, bparchive, bplist, and bprestore commands on the client may also be useful for debugging problems with xbp.
xbpadm	Administrator utility for backup policy management that runs on a UNIX master server. This utility has options for configuring and managing NetBackup. It has an X Windows based, graphical interface and is functionally very similar to the menu version, bpadm. **Started By:** /usr/openv/netbackup/bin/xbpadm command on the master server. (VERITAS recommends that you use xbpadm only on the master server.) **Stopped By:** Quit option in xbpadm. **Activity Log:** /usr/openv/netbackup/logs/xbpadm.
xbpmon	Available only on UNIX. The job monitor is a utility for monitoring the progress of backup and archive jobs. It also provides limited job control. The jnbSA and the NetBackup Windows NT/2000 administration interfaces have an equivalent utility called the Activity monitor. **Started By:** From xbpadm or with the /usr/openv/netbackup/bin/xbpmon command. **Stopped By:** Quit option from within xbpmon. **Activity Log:** /usr/openv/netbackup/logs/xbpmon.

NetBackup Databases

Table 8 describes the NetBackup databases. These databases contain information that is used internally by NetBackup and reside in the `/usr/openv/netbackup/db` directory on UNIX servers and in the *install_path*`\NetBackup\db` directory on Windows NT/2000 NetBackup servers.

Table 8. NetBackup Databases

Database	Contents
config	Configuration information. This database resides on the master server and has three parts: `class`: Contains information about each NetBackup class. `config`: Contains information about global attributes, storage units, and database backups. `altnames`: Contains information about alternate client names for restores.
error	Error and status information about NetBackup operations. This database resides on the master server and has two parts: `error`: Contains information recorded during backup operations and used in the NetBackup reports. `failure_history`: Contains daily history of backup errors.
images	Information about the backup images and resides only on the master server. One of the files in the `images` directory is the `file` database. The `file` database is the one that NetBackup accesses when a user browses for files to restore.
jobs	Job information that is used by the NetBackup job monitor (UNIX NetBackup server) and activity monitor (Windows NT/2000 NetBackup server). The Jobs database is on the master server
media	Media related information used by `bptm`. Each master or media server has a media database with media information for the images stored on that server's storage units. The media database also has an errors file that contains error history information for media and devices.

Media Manager Functional Description

This section explains the operation of Media Manager software and contains the following discussions:

- Startup Process
- Media and Device Management Process

- Barcode Operations
- Media Manager Components

Note In this section, the term Media Manager refers to the media and device management software that is part of NetBackup on either a UNIX or Windows NT/2000 NetBackup server.

Startup Process

Media Manager is part of NetBackup but, on UNIX, can also be run independently and used by other applications, such as Storage Migrator. The easiest way to start Media Manager is to initiate all the necessary processes during system startup on all servers that have devices under control of Media Manager.

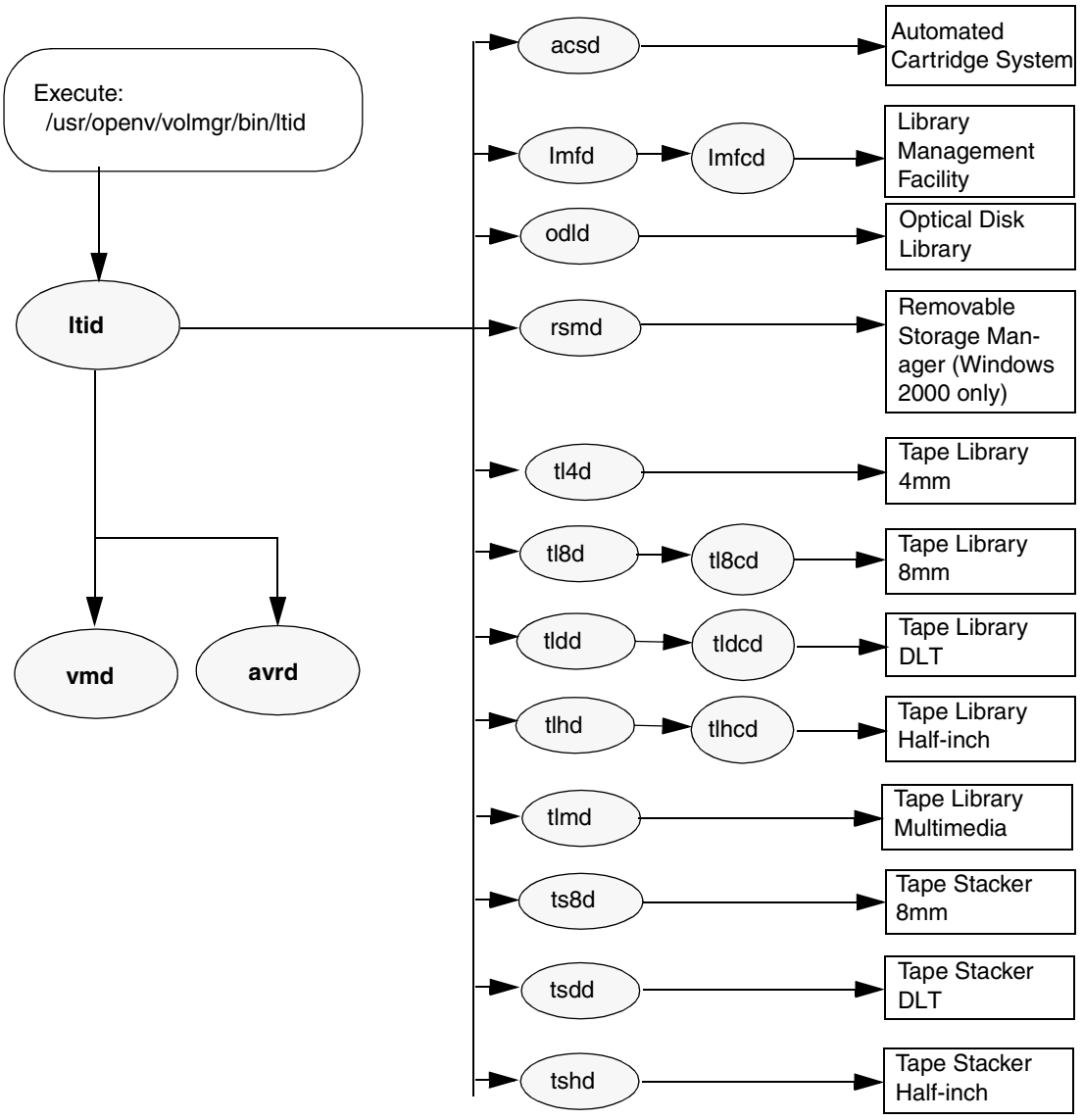
`ltid` automatically starts other daemons and programs as necessary. Figure 14 shows the Media Manager daemons that should be running after initial startup. In the case of robotic daemons, such as `ts8d` and `rsmd`, the associated robot must also be configured for the daemon to run. See Table 10 for other ways to start and stop these daemons.

As shown on Figure 14, the LMF, TL8, TLH, and TLD, require two types of daemons: robotic and robotic control.

- Each host with a drive attached must have a robotic daemon. These daemons provide the interface between `ltid` and the robot or, if different drives within a robot can attach to different hosts, the robotic daemon communicates with a robotic-control daemon (see below).
- Robotic-control daemons centralize the control of robots when drives within a robot can connect to different hosts. A robotic-control daemon receives mount and unmount requests from the robotic daemon on the host to which the drive is attached and then communicates these requests to the robot.

You must know the hosts involved in order to start all the daemons for a robot.

Figure 14. Starting Media Manager



Media and Device Management Process

When the Media Manager daemons are running, NetBackup, Storage Migrator (UNIX only), or other users can initiate data storage or retrieval by sending a request for the required media ID to the Media Manager device daemon, `ltid` (Figure 15). `ltid` determines the location of the requested media ID by sending a query to the Media Manager volume daemon, `vmd`. The volume daemon then returns the information it has about the media, including: robot number, robot type, host, slot, and barcode.

If the media is in a robot, `ltid` sends a mount request to the robotic daemon that controls the robot. The robotic daemon then chooses an available drive, mounts the media, and sets a drive busy status in memory shared by itself and `ltid`. If it receives another mount request, `ltid` checks that status to determine which (if any) drives are available. Drive busy status also appears in the Device Monitor (and `xdevadm`).

Assuming that the media is physically in the robot, the media is mounted and the operation proceeds. If the media is not in the robot, `ltid` sends a mount request, which appears as a pending request in the Device Monitor (and `xdevadm`). An operator must then insert the media in the robot and use the appropriate Device Monitor (or `xdevadm`) command to resubmit the request so the mount request can occur.

A mount request is also issued if the media is for a nonrobotic (standalone) drive and the drive does not contain media that meets the criteria in the request. If the request is from NetBackup and the drive does contain appropriate media, then that media is automatically assigned and the operation proceeds. See the *NetBackup System Administrator's Guide* for more information on NetBackup media selection for nonrobotic drives.

When a robotic volume is added or removed through a mailslot (or inport/outport), the media management utility communicates with the appropriate robotic daemon to verify the volume location and/or barcode. The media management utility (through a library or command-line interface) also calls the robotic daemon for robot inventory operations

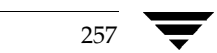
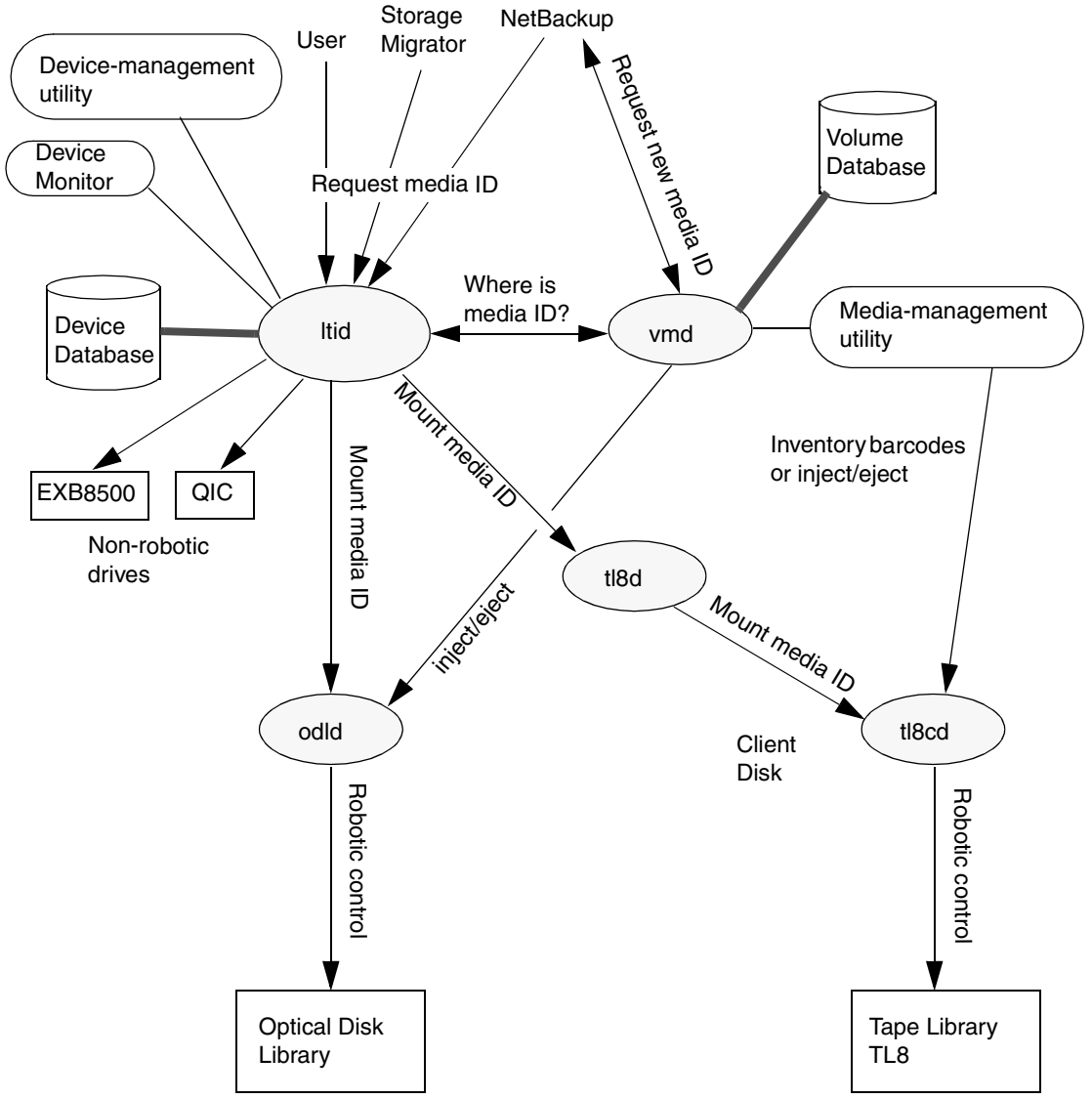


Figure 15. Media and Device Management Example Process



Barcode Operations

Barcode reading is mainly a function of the robot hardware rather than Media Manager. When a robot has a barcode reader, it scans any barcode that may be on a tape and stores the code in its internal memory. This associates the slot number and the barcode of the tape in that slot. Media Manager determines that association for its own use by interrogating the robot.

If a robot supports barcodes, Media Manager automatically compares a tape's barcode to what is in the volume database as an extra measure of verification before mounting the tape.

Media Requests Involving Barcodes

A request for media that is in a robot that can read barcodes begins in the same manner as other requests (see Figure 16). The Media Manager device daemon, `ltid`, determines the location of the requested media ID by querying the Media Manager volume daemon, `vmd`. The volume daemon then returns the information it has about the media, including: robot number, robot type, host, slot, and barcode.

`ltid` includes the media ID and location information in a mount request to the robotic daemon for the robot that has the media ID. This request causes the robotic daemon to query the robot for the barcode of the tape in the designated slot (preliminary check to see if the correct media is in the slot). The robot returns the barcode value it has in memory to the robotic daemon, which compares this barcode with the value it received from `ltid`:

- If the barcodes don't match, the robotic daemon informs `ltid` and a pending action request (Misplaced Tape) appears in the Device Monitor (and `xdevadm`). An operator must then insert the correct tape in the slot.
- If the barcodes match, the robotic daemon requests the robot to move the tape to a drive. The robot then mounts the tape. At the start of the operation, the application (for example, NetBackup) checks the media ID and if it also matches what should be in this slot, the operation proceeds. For NetBackup, a wrong media ID, results in a *Media Manager Found Wrong Tape in Drive* error (status code 93).

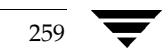
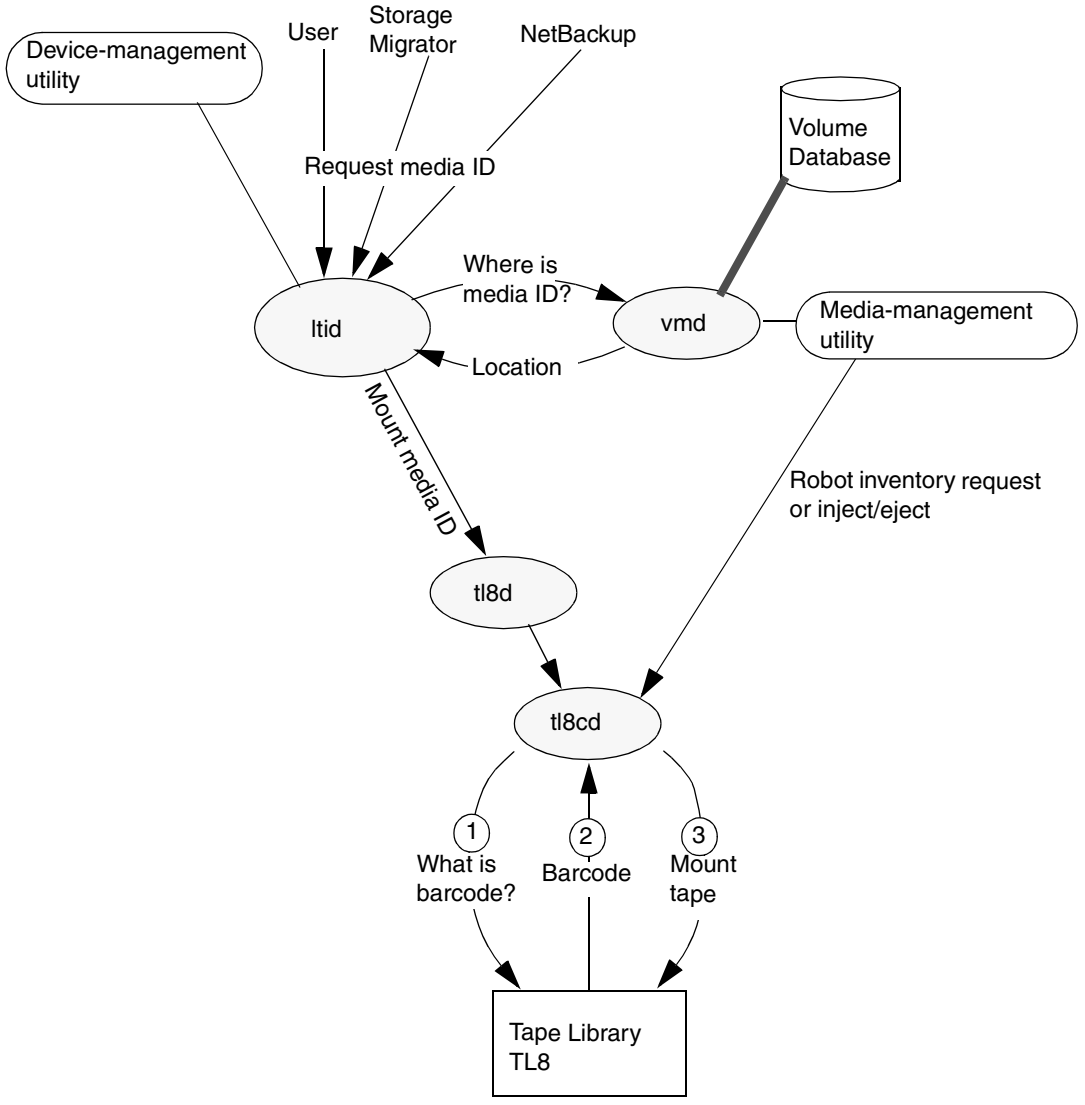


Figure 16. Barcode Request



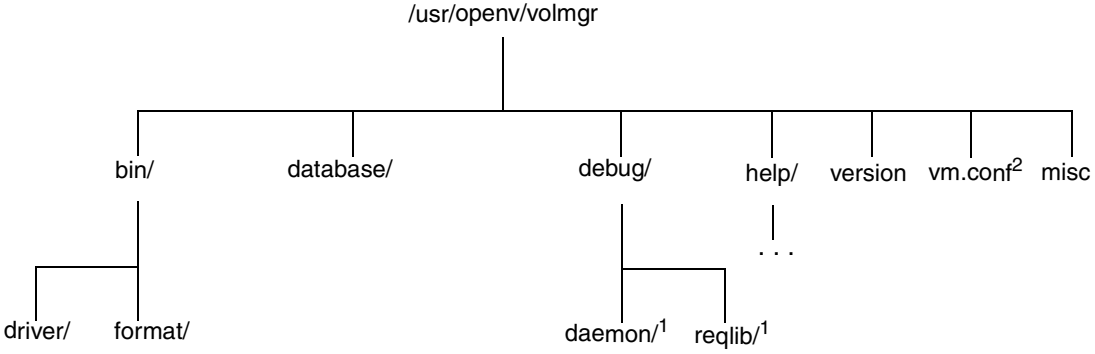
Media Manager Components

Media Manager Directories and Files

Figure 17 shows the file and directory structure for Media Manager on a UNIX server. A Windows NT/2000 NetBackup server has equivalent files and directories that are located in the directory where NetBackup is installed (`c:\Veritas` by default).

Table 9 describes the directories and files that are of special interest.

Figure 17. Media Manager Directories and Files



1 Created by administrator to enable vmd debug logging.
2 Created by administrator or automatically by media management utilities.

Caution *DO NOT* under any circumstances attempt to modify the Media Manager databases. These files are for internal program use only and changing them will result in program failure and possible loss of data. It is also recommended that you do not move them to another host.

Table 9. Media Manager Directories and Files

File or Directory	Contents
`bin`	Commands, scripts, programs, daemons, and files required for Media Manager operation and administration. There are two subdirectories under bin. driver: Contains SCSI drivers used on various platforms to control robotics. format: Disk format information for optical platters on Solaris platforms. goodies: Contains Motif interfaces (`xdevadm`, `xvmadm`) on UNIX platforms where Java is supported.
`database`	Media Manager databases contain information about the drives, robots, and media that are under Media Manager control. The volume database that usually resides on the master server contains volume information for multiple media servers.
`debug`	Debug logs for the Media Manager volume daemon, `vmd`, and all requesters of `vmd`. The administrator must create these directories (daemon and reqlib) for debug logging to occur.
`help`	Help files used by Media Manager programs. These files are in ASCII format.
`version`	Version and release date of the software.
`vm.conf`	Media manager configuration options.
`misc`	Lock files and temporary files required by various components of Media Manager.

Programs and Daemons

Table 10 describes the Media Manager programs and daemons. The explanations include what starts and stops the program or daemon, and the log (if any) where it records its activities. On UNIX, all of the components discussed in this table reside under `/usr/openv/volmgr/bin`. On Windows NT/2000, they reside under *install_path*`\volmgr\bin`.

Table 10. Media Manager Daemons and Programs

Program/ Daemon	Description
acssel	Available only on UNIX. See the *Media Manager System Administrator's Guide* (UNIX or Windows NT/2000) for details.
acsssi	Available only on UNIX. See the *Media Manager System Administrator's Guide* (UNIX or Windows NT/2000) for details.
ascd	The Automated Cartridge System Software daemon interfaces with the Automated Cartridge System and communicates with the server that controls the ACS robotics. Also, for UNIX see the acsssi and acssel programs. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/ascd command. **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid) or by putting VERBOSE in the vm.conf file.
avrd	The automatic-volume-recognition daemon controls automatic volume assignment and label scanning. This lets Media Manager read labeled tape and optical disk volumes and to automatically assign the associated removable media to requesting processes. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/avrd command). **Stopped By:** Stopping ltid, (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by aborting avrd and starting the daemon with the -v option.

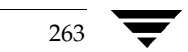


Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
lmfd	The Library Management Facility daemon works in conjunction with lmfcd to handle requests to robots controlled by a Fujitsu Library Management Facility (LMF). lmfd provides the interface between the local ltid and the robotic control (lmfcd) in the same manner as explained later for tl8d. This robot is not available on Windows NT/2000. **Started By:** Starting ltid (or independently by using the /usr/openv/volmgr/bin/lmfd command). **Stopped By:** Stopping ltid or independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid) or by adding VERBOSE to the vm.conf file.
ltid	The Media Manager device daemon (NetBackup Device Manager service on Windows NT/2000) controls the reservation and assignment of tapes and optical disks. **Started By:** /usr/openv/volmgr/bin/ltid command on UNIX or Stop/Restart Device Management command in Media and Device Management window on Windows NT/2000. **Stopped By:** /usr/openv/volmgr/bin/stopltid command on UNIX or Stop/Restart Device Management command in the Media and Device Management window on Windows NT/2000. **Activity Log:** All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (available only on UNIX) or adding VERBOSE to the vm.conf file.
odld	The Optical Disk Library daemon interfaces with the Optical Disk Library, communicating with the robotics through a SCSI interface. This library is not supported on Windows NT/2000. **Started By:** Starting ltid or independently by using the /usr/openv/volmgr/bin/odld command. **Stopped By:** Stopping ltid or independently by finding the PID (process id) and then using the kill command. **Activity Log:** All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid) or adding VERBOSE to the vm.conf file.

Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
rsmd	The Tape Library RSMD daemon is the interface between ltid and the Microsoft Windows 2000 Removable Storage Manager (RSM) interface. The rsmd daemon runs only on Windows 2000 systems; note that the system must have rsm devices configured in the Media Manager interface. **Started By:** Starting ltid on Windows 2000 only. **Stopped By:** Stopping ltid on Windows 2000 only. **Activity Log:** All errors are logged in the system log. Debug information is included in the system log as notifications.
tl4d	The Tape Library 4MM daemon is the interface between ltid and the Tape Library 4MM and communicates with the robotics through a SCSI interface. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tl4d command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tl8d	The Tape Library 8MM daemon drives in the same TL8 robot may be attached to different hosts than the robotic control. tl8d is the interface between the local ltid and the robotic control. If a host has a device control file for a drive in a TL8 robot, then mount or unmount requests for that drive go first to the local ltid and then to the local tl8d (all on the same host). tl8d then forwards the request to tl8cd on the host that is controlling the robot (could be on another host). **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tl8d command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command. **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).

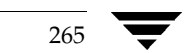


Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
tl8cd	The Tape Library 8MM Control daemon provides the robotic control for a TL8 robot and communicates with the robotics through a SCSI interface. tl8cd receives mount and unmount requests from tl8d on the host to which the drive is attached and then communicates these requests to the robot. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tl8cd command). **Stopped By:** Stopping ltid or by using the tl8cd -t command. **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tldd	The Tape Library DLT daemon works in conjunction with tldcd to handle requests to TLD robots. tldd provides the interface between the local ltid and the robotic control (tldcd) in the same manner as explained previously for tl8d. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tldcd	The Tape Library DLT Control daemon provides robotic control for a TLD robot in the same manner as explained previously for tl8cd. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldcd command). **Stopped By:** Stopping ltid or by using the tldcd -t command. Stopping ltid or tldd does not stop tldcd since it may be in use by tldd on another host. **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).

Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
tlhd	The Tape Library Half-inch daemon works in conjunction with tlhcd to handle requests to TLH robots that are in an IBM Automated Tape Library (ATL). tlhd provides the interface between the local ltid and the robotic control (tlhcd) in the same manner as explained previously for tl8d. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tlhd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tlhcd	The Tape Library Half-inch Control daemon provides robotic control for a TLH robot that is in an IBM Automated Tape Library (ATL) in a similar manner to that which was explained previously for tl8cd. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldcd command). **Stopped By:** Stopping ltid or by using the tlhcd -t command. **Activity Log:** All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.
tlmd	The Tape Library Multimedia daemon is the interface between ltid and a TLM robot that is in an EMASS Distributed AML Server (DAS). This daemon communicates with the TLM robotics through a network API interface. This robot is not supported on Windows NT/2000. **Started By:** Starting ltid or independently by using the /usr/openv/volmgr/bin/tlmd command. **Stopped By:** Stopping ltid or independently by finding the PID (process id) and then using the kill command. **Activity Log:** All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.

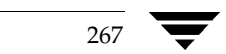


Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
tpconfig	tpconfig is a command line administrator utility for configuring devices under Media Manager. The graphical user interfaces provide equivalent functionality. **Started By:** tpconfig command. **Stopped By:** Quit option from within the utility on UNIX. On Windows NT/2000, tpconfig is a command-line interface that runs to completion (no quit option). **Activity Log:** None
tsdd	The Tape Stacker DLT daemon is the interface between ltid and the DLT tape stacker and communicates with the robotics through a SCSI interface. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tsdd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tshd	The Tape Stacker Half-inch daemon is the interface between ltid and the half-inch-cartridge stacker and communicates with the robotics through a SCSI interface. This robot is not supported on Windows NT/2000. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tshd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).

Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
ts8d	The Tape Stacker 8MM daemon is the interface between ltid and the 8-mm Tape Stacker and communicates with the robotics through a SCSI interface. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/ts8d command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Activity Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the Media Manager configuration file, vm.conf. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
vmd	The Media Manager volume daemon (NetBackup Volume Manager service on Windows NT/2000) manages the volume database, provides ltid with the location of requested volumes, and keeps track of the number of mounts and last mount time for each volume. **Started By:** Starting ltid (or on UNIX, independently by using the Initiate Media Manager Volume daemon option in vmadm) **Stopped By:** Terminate Media Manager Volume Daemon option in vmadm). **Activity Log:** System log and also a debug log if the daemon or reqlib debug directories exist (see "Activity Logs" on page 47).
vmadm	Available only on UNIX. An administrator utility with options for configuring and managing volumes under control of Media Manager. It has a menu-driven, character-based interface that can be used from workstations that do not have X Windows capabilities. **Started By:** /usr/openv/volmgr/bin/vmadm command **Stopped By:** Quit option from within the utility. **Activity Log:** /usr/openv/volmgr/debug/reqlib
xdevadm	Available only on UNIX. An administrator utility with options for configuring and managing devices under Media Manager. It has an X Windows based, graphical interface and provides all the functionality of tpconfig. **Started By:** /usr/openv/volmgr/bin/xdevadm command or the Device Management option from the xbpadm or xvmadm File menu. **Stopped By:** Quit option in xdevadm. **Activity Log:** /usr/openv/volmgr/debug/reqlib

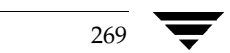


Table 10. Media Manager Daemons and Programs (continued)

Program/ Daemon	Description
xvmadm	Available only on UNIX. An administrator utility with options for configuring and managing volumes under Media Manager. It has an X Windows based, graphical interface and provides all the functionality of vmadm. **Started By:** /usr/openv/volmgr/bin/xvmadm command or the Volume Management option from the xdevadm File menu. **Stopped By:** Quit option in xvmadm. **Activity Log:** /usr/openv/volmgr/debug/xvmadm

Networks and Hostnames B

In a configuration with multiple networks and clients with more than one hostname, the NetBackup administrator must configure the class entries carefully, at all times considering the network configuration (physical, hostnames and aliases, NIS/DNS, routing tables, and so on). This is especially true if the desire is to direct backup and restore data across specific network paths.

For a backup, NetBackup connects to the host name as configured in the class. The operating system's network code resolves this name and sends the connection across the network path defined by the system's routing tables. The `bp.conf` file is not a factor in determining this.

For restores from the client, the client connects to the master server. For example, on a UNIX system, the master server is the first one named in the `/usr/openv/netbackup/bp.conf` file. On a Windows system, the master server is specified on the Servers tab of the Specify NetBackup Machines dialog box (to open this dialog, start the NetBackup client user interface and click Specify NetBackup Machines on the Actions menu). The network path to the server is determined by the client's network code that maps the server name to an IP address.

Upon receipt of the connection, the server determines the client's configured name from the *peername* of its connection to the server.

The peername is derived from the IP address of the connection. This means that the address must translate into a host name (using the `gethostbyaddr()` network routine). This name is visible in the `bprd` activity log when a connection is made as in the line:

```
Connection from host peername ipaddress ...
```

The client's configured name is then derived from the *peername* by querying the `bpdbm` process.

The `bpdbm` process compares the peername to a list of client names generated from:

1. All clients for which a backup has been attempted

   and

2. All clients in all classes

The comparison is first a simple string comparison which, if successful, is verified by comparing hostnames and aliases retrieved by using the network function `gethostbyname()`.

If none of the comparisons succeed, a more brute force method is used, which compares all names and aliases using `gethostbyname()`.

The configured name is the first comparison that succeeds. Note that other comparisons might also have succeeded if aliases or other "network names" are configured.

If the comparison fails, the client's hostname as returned by the `gethostname()` function on the client is used as the configured name. One example of why the comparison could fail is the case where the client had changed its hostname but its new hostname is not reflected in any classes yet.

These comparisons are logged in the `bpdbm` activity log if `VERBOSE` is set. You can determine a client's configured name by using the `bpclntcmd` command on the client. For example:

`# /usr/openv/netbackup/bin/bpclntcmd -pn` (UNIX)

`#` *install_path*`\NetBackup\bin\bpclntcmd -pn` (Window NT/2000)

```
expecting response from server wind.abc.me.com
danr.abc.me.com danr 194.133.172.3 4823
```

Where the first output line identifies the server to which the request is directed and the second output line is the server's response in the following order:

- Peername of the connection to the server
- Configured name of the client
- IP address of the connection to the server
- Port number used in the connection

When the client connects to the server, it sends three names to the server:

- *browse client*
- *requesting client*
- *destination client*

The *browse client* name is used to identify the client files to list or restore from. The user on the client can modify this name to restore files from another client. For example, on a Windows NT/2000 client, the user can change the client name by using the client user interface (see the user's guide for instructions). For this to work, however, the administrator must also have made a corresponding change on the server (see "Allowing Alternate Client Restores" in the *NetBackup System Administrator's Guide - UNIX*).

The *requesting client* is the value from the `gethostname()` function on the client.

The *destination client* name is a factor only if an administrator is pushing a restore to a client from a server. For a user restore, *destination client* and *requesting client* are the same. For an administrator restore, the administrator can specify a different name for the destination client.

By the time these names appear in the `bprd` activity log, the requesting client name has been translated into the client's configured name.

Depending on the particulars of the restore request (for example, from root on a server, from a client, to an alternate client, and so on), the name used to connect back to the client to complete the restore is either the client's peername or its configured name.

When modifying client names in NetBackup classes to accommodate specific network paths, the administrator needs to consider:

- The client name as configured on the client. For example, on UNIX this is `CLIENT_NAME` in the client's `bp.conf` file. On a Windows client, it is on the General tab of the NetBackup Configuration dialog box. To open this dialog box, click Configure on the Actions menu in the Backup, Archive, and Restore interface.
- The client as currently named in the class configuration.
- Existing client backup and archive images as recorded in the `images` directory on the master server. On a UNIX server, this is the `/usr/openv/netbackup/db/images` directory. On a Windows NT/2000 NetBackup server this is the *install_path*`\NetBackup\db\images` directory.

All of the above can require manual modification by the administrator if a client has multiple network connections to the server and restores from the client fail due to a connection-related problem.

On UNIX, the public domain program `traceroute` (not included with NetBackup) often can provide valuable information about a network's configuration. Some system vendors include this program with their systems.

If Domain Name Services are used and the (possibly unqualified) name that the NetBackup client obtains through its `gethostname()` library function is unknown to the Domain Name Service (DNS) on the master server, the master server can be unable to reply to client requests. Whether this situation exists, depends on how the client and the server are configured. If `gethostname()` on the client returns host names that are not qualified to the extent that DNS on the master server can resolve them, then you will encounter problems.

Although a possible solution is to reconfigure the client or the master server DNS hosts file, this is not always desirable. For this reason, NetBackup provides a special file on the master server. This file is:

`/usr/openv/netbackup/db/altnames/host.xlate` (UNIX)

install_path`\NetBackup\db\altnames\host.xlate` (Windows NT/2000)

You can create and edit this file to force the desired translation of NetBackup client host names.

Each line in the `host.xlate` file has three elements: a numeric key and two hostnames. Each line is left-justified, and each element of the line is separated by a space character.

key hostname_from_ client client_as_known_by_server

Where

- *key* is a numeric value used by NetBackup to specify the cases where the translation is to be done. Currently this value must always be 0, indicating a configured name translation.
- *hostname_from_client* is the value to translate. This must correspond to the name that is obtained by the client's `gethostname()` function and sent to the server in the request.
- *client_as_known_by_server* is the name to substitute for *hostname_from_client* when responding to requests. This name must be the name configured in the NetBackup configuration on the master server and must also be known to the master server's network services.

For example, the line

```
0 danr danr.eng.aaa.com
```

specifies that when the master server receives a request for a configured client name (numeric key 0), the name danr is always replaced by the name danr.eng.aaa.com. This resolves the problem mentioned above, assuming that:

- The client's `gethostname()` function returned danr.
- The master server's network services `gethostbyname()` function did not recognize the name danr.
- The client was configured and named in the NetBackup configuration as danr.eng.aaa.com and this name is also known to network services on the master server.

Robotic Test Utilities C

Each of the robotic software packages includes a robotic test utility for communicating directly with robotic peripherals. The tests are for diagnostic purposes and the only documentation is the online help that you can view by entering a question mark (?) after starting the utility. Specify `-h` to display the usage message.

Note Do not use the robotic test utilities when backups or restores are active. The tests lock the robotic control path and prevent the corresponding robotic software from performing actions, such as loading and unloading media. If a mount is requested, the corresponding robotic process times out and goes to the DOWN state. This usually results in a media mount timeout. Also, be certain to quit the utility when your testing is complete.

Robotic Tests on UNIX

If the robot has been configured (that is, added to the Media Manager device database), start the robotic test utility by using the `robtest` command. This saves time, since robotic and drive device paths are passed to the test utility automatically. The procedure is as follows:

1. Execute the following command:

   `/usr/openv/volmgr/bin/robtest`

   The test utility menu appears.

2. Select a robot and press Enter.

   The test starts.

If the robot is not configured, you cannot use `robtest` and must execute the command that applies to the robot you are testing.

ACS

`/usr/openv/volmgr/bin/acstest -r` *ACSLS_HOST*

LMF

`/usr/openv/volmgr/bin/lmftest -r` *robotic_library_name*

ODL

```
/usr/openv/volmgr/bin/odltest -r roboticpath
```

TL4

```
/usr/openv/volmgr/bin/tl4test -r roboticpath
```

TL8

```
/usr/openv/volmgr/bin/tl8test -r roboticpath
```

TLD

```
/usr/openv/volmgr/bin/tldtest -r roboticpath
```

TLH

```
/usr/openv/volmgr/bin/tlhtest -r robotic_library_path
```

TLM

```
/usr/openv/volmgr/bin/tlmtest -r DAS_Hostname
```

TS8

```
/usr/openv/volmgr/bin/ts8test -r roboticpath
```

TSD

```
/usr/openv/volmgr/bin/tsdtest -r roboticpath
```

TSH

```
/usr/openv/volmgr/bin/tshtest -r roboticpath
```

Note For more information on ACS, TLH, LMF, and TLM robotic control, see the appendixes in the *Media Manager System Administrator's Guide - UNIX*.

For more information on RSM robotic control, refer to the Robot Drive appendix in the *Media Manager System Administrator's Guide - Windows NT/2000*.

In the above commands, *roboticpath* is the full path to the device file for the robotic control (SCSI). Refer to the *Media Manager Device Configuration Guide* and review the chapter for your platform to find the appropriate value for *roboticpath*.

There is also an optional parameter that specifies the device file path for the drive(s) so that SCSI unloading of the drive(s) can be done with this utility.

Robotic Tests on Windows NT/2000

If the robot has been configured (that is, added to the Media Manager device database), start the robotic test utility by using the `robtest` command. This saves time, since robotic and drive device paths are passed to the test utility automatically. The procedure is as follows:

1. Execute the following command:

   ***install_path*\Volmgr\bin\robtest.exe**

   The test utility menu appears.

2. Select a robot and press Enter.

   The test starts.

Note If the robot is not configured, you cannot use `robtest` and must execute the command that applies to the robot you are testing (see below). However, in the case of an RSM robot, the robot *must* be configured under NetBackup before a test can be run. When the RSM robot has been configured, use the `robtest` command as described above.

ACS

install_path`\Volmgr\bin\acstest -r` *ACSLS_HOST*

TL4

install_path`\Volmgr\bin\tl4test -r` *roboticpath*

TL8

install_path`\Volmgr\bin\tl8test -r` *roboticpath*

TLD

install_path`\Volmgr\bin\tldtest -r` *roboticpath*

TLH

install_path`\Volmgr\bin\tlhtest -r` *robotic_library_name*

TS8

install_path`\Volmgr\bin\ts8test -r` *roboticpath*

TSD

install_path`\Volmgr\bin\tsdtest -r` *roboticpath*

Glossary

access control list (ACL)

Security information associated with files on some file systems.

ACS

Automated Cartridge System. This robot type is supported only by NetBackup DataCenter servers.

active job

A job for which NetBackup is currently processing backup or restore data.

activity logs

Logs that can be optionally enabled for specific NetBackup programs and processes and then used to investigate problems.

activity monitor

A NetBackup administration utility that displays information about NetBackup jobs and provides limited control over them.

administrator

A user that is granted special privileges to install, configure, and manage the operation of a system, network, or application

administration client

A Windows NT/2000 NetBackup client that has the administration interface software installed and can be used to administer NetBackup servers.

AIT

Sony Advanced Intelligent Tape, a type of tape drive or media type.

alternate-client restore

Restoring files to your client when they were originally backed up from a different client. The administrator using the interface on the master server can direct a restore to any client (this variation is called a server directed restore).

alternate-target restore

On a Novell NetWare server platform running the NetBackup target version of client software, this operation restores files to a different target than the one from which they were backed up.

alternate path restore

Restores files to a different directory than the one from which they were backed up.

archive

A special kind of backup where NetBackup backs up the selected files, and if the backup is successful, deletes the files from the local disk. In this manual, references to backups also apply to the backup portion of archive operations except where otherwise noted.

archive bit

A file-status bit that the Microsoft based operating system sets when it writes a file, thereby indicating that the file has changed.

attributes for a class

Configuration parameters that control the behavior of NetBackup during operations involving this class.

automatic backup

A scheduled backup by the master server.

back up

The act of copying and saving files and folders to storage media.

backup

Refers to the process of copying and saving files and directories to storage media. For example, *the backup is complete*. This term can also refer to the collection of data that NetBackup saves for a client during a backup or archive. For example, *duplicate the backup*.

Backup is two words when used as a verb. For example, *back up the file*.

backup, archive, and restore interface

The name of the NetBackup Microsoft Windows and Java based user interfaces for clients. On servers, these interfaces can be started through the NetBackup Administration interface.

backup window

The period of time during which backups can begin.

block size

The number of bytes in each block of data written on the media during a backup.

bp

A backup, archive, and restore utility for users on NetBackup UNIX clients. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bpadm

An administrator utility that runs on NetBackup UNIX servers. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bp.conf file

A NetBackup configuration file on UNIX servers and also on UNIX, Macintosh, and OS/2 clients.

bp.ini file

NetBackup initialization file for Novell NetWare target clients.

bpcd

NetBackup Client service on Windows NT/2000 and the NetBackup Client daemon on UNIX.

bprd

NetBackup Request Manager service on Windows NT/2000 and NetBackup Request daemon on UNIX.

catalogs

Internal NetBackup and Media Manager databases. These catalogs contain information about configuration, media, devices, status, errors, and the files and directories in the stored backup images.

CDF

Context-dependent file, which is a type of directory structure on a Hewlett-Packard system.

class

Defines the backup policy for a group of one or more clients that have similar backup requirements.

client

The system with the files to back up, archive, or restore.

client-user interface

The program used to perform user backups, archives, and restores.

cluster

See master and media server cluster.

command lines

Commands that users can execute either from the system prompt or in scripts.

compression

The process of compacting data to enable more efficient transmission and storage.

configuration

The parameters that govern the behavior of an application. This term can also refer to the manner in which a network or system is laid out or connected (for example, a network configuration).

cpio

A UNIX command for formatting data on a tape.

ctime

The time that a UNIX inode was changed.

cumulative-incremental backup

A backup that is scheduled by the administrator on the master server and backs up files that have changed since the last successful full backup. All files are backed up if no prior backup has been done. Also see "differential-incremental backup."

daemon

A program on a UNIX system that runs in the background and performs some task (for example, starting other programs when they are needed). Daemons are generally referred to as services or processes on Windows NT/2000 systems.

database-agent clients

Clients with additional NetBackup software that is designed to back up relational databases.

database-extension clients

See "database-agent clients."

debug logs

See "activity logs."

device delays

Delays caused by the device that are beyond the control of the storage application. An example is the time required to position tape under the read and write heads.

device host

A Media Manager host where a drive or robotic control is attached or is defined.

device monitor

A Media Manager administration utility that provides monitoring and manual control of Media Manager storage devices. For example, an administrator or computer room operator can use this utility to manually reset devices or set them to the UP or DOWN state.

DHCP

Dynamic host configuration protocol. This TCP/IP protocol automatically assigns temporary IP addresses to hosts when they connect to the network.

differential-incremental backup

Scheduled by the administrator on the master server and backs up files that have changed since the last successful incremental or full backup. All files are backed up if no prior backup has been done. Also see "cumulative-incremental backup."

directory depth

The number of levels below the current directory level that the NetBackup interfaces show in their directory and file list displays.

directory tree

The hierarchical structure in which files are organized on a disk. Each directory lists the files and directories that are directly below it in the tree. On UNIX, the topmost directory is called the root directory.

disaster recovery

Recovering data from backups after a disk crash or other catastrophe.

disk

Magnetic or optical disk storage media.

disk-image backup

A bit-by-bit rather than a file system backup of a disk drive on Windows NT/2000.

DLT

Digital-linear tape or tape drive type.

Domain Name Service (DNS)

A program that handles name translation for network communications.

drive cleaning

The use of a special cleaning tape to clean the heads on a drive.

duplicate image

A copy of a backup image.

encryption

Provides additional security by encrypting backup data on the client. This capability is available only with the NetBackup Encryption option.

entry and exit ports

A slot or other opening in a robot where you can insert or remove a tape without having to access the interior of the robot. After inserting a tape, you move it to a slot by using an inject command. Prior to removing a tape, you move it to the port by using an eject command. The inject and eject commands are supported through the add and move screens in the Media Manager administration interface. Entry and exit ports are sometimes called mailslots, or inports and outports.

exclude list

A list that designates files or directories to exclude from automatic backups.

expiration (image)

The date and time when NetBackup stops tracking a backup image.

expiration (volume)

The date and time when the physical media (tape) is considered to be no longer usable.

EVSN

External volume serial number. This is an identifier written on a media cartridge or canister so the operator can identify the volume before inserting it into a drive or robot. For labeled media, the EVSN must be the same as the RVSN (identifier recorded on the media). For all media, the EVSN is the same as the media ID.

FastBackup

A special type of raw-partition backup that can be performed only on an Auspex client (this option is available only for NetBackup DataCenter).

FlashBackup

A special type of raw-partition backup that requires the NetBackup FlashBackup separately-priced option (this option is available only for NetBackup DataCenter).

flush level

Controls how often Netbackup clears its log files on a Novell NetWare or Microsoft Windows client platform.

fragment

A part of a backup or archive image. NetBackup can be configured to divide images into fragments when they exceed a certain size or span tapes.

frequency (backup)

How often NetBackup performs scheduled backups. For example, if the frequency is seven days then backups occur once a week.

FROZEN media state

If a volume is FROZEN, NetBackup keeps it indefinitely and can restore from it but not use it for further backups or archives.

full backup

A backup that copies, to a storage unit, all files and directories that are beneath a specified directory.

FULL media state

If this appears in a report or listing, it indicates the volume is FULL and cannot hold more data or be used for further backups.

global attributes

NetBackup configuration attributes that affect all classes.

Global Data Manager

A separately-priced option (for UNIX servers) that provides an interface with a tree view where the administrator can view and administer multiple master servers. The server where the option is installed is called a Master of Masters.

GNU tar

A public domain version of the UNIX tar program.

goodies directory

A directory containing programs, scripts, and other files that are not formally supported.

gravity stacker

A robot that relies on gravity to advance to the next required tape.

GUI

Graphical user interface.

hard link

On UNIX, a hard link is a pointer to the inode for the data. On Windows NT/2000 a hard link is a directory entry for a file. Every file can be considered to have at least one hard link. On NTFS volumes each file can have mulitple hard links, and a single file can appear in many directories (or even in the same directory with different names).

heap level

A parameter for memory-heap debugging on a Novell NetWare or Windows NetBackup client.

hierarchical storage management

The process of automatically migrating selected files from a managed file system to specified migration levels on secondary storage, while maintaining transparent access to those files.

host

A computer that executes application programs.

host name

Name by which a host computer is identified by programs and other computers in the network.

HSM

See storage migrator.

image

The collection of data that NetBackup saves for an individual client during each backup or archive. The image contains all the files, directories, and catalog information associated with the backup or archive.

import

The process of recreating NetBackup records of images so the images can be restored.

include list

A list that designates files or directories to add back in from the exclude list.

incremental backup

See "cumulative-incremental backup" and "differential-incremental backup."

inport

See "entry and exit ports."

inode

A UNIX data structure that defines the existence of a single file.

install_path

Directory where NetBackup and Media Manager software is installed. The default on Windows NT/2000 is `C:\Program Files\VERITAS` and on UNIX it is `/usr/openv`.

jbpSA

The Java-based NetBackup interface for performing user backups, archives, and restores.

jnbSA

The Java-based NetBackup interface for administrators.

job

A parcel of work submitted to a computer. NetBackup jobs are backups, archives, or restores.

kernel

The nucleus of an operating system.

keyword phrase

A textual description of a backup.

kill a job

Terminating a job and removing it from the job queue.

label

Identifier of a tape or optical disk volume. A recorded label includes a media ID.

A barcode label allows a barcode scanner to be used for media tracking.

library

Refers to a robot and its accompanying software. A library includes a collection of tapes or optical platters used for data storage and retrieval. For example, a Tape Library DLT (TLD) refers to a robot that has TLD robotic control.

link

See "hard link" or "symbolic link."

LMF - Library Management Facility

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

This robot type is supported only by NetBackup DataCenter servers.

load

(noun) Amount of work that is being performed by a system or the level of traffic on a network. For example, network load affects performance.

(verb) Copy data to internal memory. For example, load the installation program.

logs

Files where a computer or application records information about its activities.

mailslot

See "entry and exit ports."

man pages

Online documentation provided with UNIX computer systems and applications.

Master and media server cluster

A NetBackup master server and the remote media servers that it is using for additional storage. It is possible to configure clusters only with NetBackup DataCenter servers. NetBackup BusinesServer supports only a single server, the master.

Master of Masters

A NetBackup host where Global Data Manager software is installed. When logging into this host, the interface has a tree view where the administrator can view and administer multiple master servers.

master server

The NetBackup server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster. NetBackup BusinesServer supports only a single server and it is the master.

media

Physical magnetic tapes, optical disks, or magnetic disks where data are stored.

media host

NetBackup server to which the job (client) is sending the data.

media ID

An identifier that is written on a volume as part of the recorded label.

Media Manager

Software that is part of NetBackup and manages the storage devices and removable media.

Media Manager Host

A host where Media Manager software is installed.

media server

A NetBackup server that provides storage within a master and media server cluster. The master can also be a media server. A media server that is not the master is called a remote media server (or slave server). NetBackup BusinesServer does not support remote media servers.

menu interface

A character-based interface for use on terminals that do not have graphical capabilities.

MHD

See "multihosted drives."

mount

Make a volume available for reading or writing.

mount point

The point where a file system on a disk logically connects to a system's directory structure so the file system is available to users and applications.

MPX

See "multiplexing."

mtime

The point in time when a UNIX or NTFS file is modified.

multihosted drives

A separately priced VERITAS option (Shared Storage Option or SSO) that allows tape drives (standalone or in a robotic library) to be dynamically shared among multiple NetBackup and Storage Migrator servers.

This option is supported only on NetBackup DataCenter servers.

multiplexing

The process of sending concurrent-multiple backups from one or more clients to a single storage device and interleaving those images onto the media.

multiplexed group

A set of backups that were multiplexed together in a single multiplexing session.

NDMP

Network data management protocol. NetBackup requires the NetBackup for NDMP separately-priced option to support NDMP.

NetBackup Client service

NetBackup Windows NT/2000 service that runs on clients and servers and listens for connections from NetBackup servers and clients in the network. When a connection is made, this service starts the necessary programs.

NetBackup configuration options

On UNIX servers and on UNIX and Macintosh, clients, these settings are made in the `bp.conf` file. On NetWare target and OS/2 clients, they are in the `bp.ini` file. On Windows NT/2000 servers and Microsoft Windows clients, these settings are called properties and are made through the Backup, Archive, and Restore interface or the Configure - NetBackup window in the administration interface.

NetBackup databases

See catalogs.

NetBackup Database Manager service

NetBackup Windows NT/2000 service that runs on the master server and manages the NetBackup internal databases (called catalogs). This service must be running on the master server during all NetBackup administrative operations.

NetBackup Device Manager service

The NetBackup Windows NT/2000 service that runs on a NetBackup server and starts the robotic control processes and controls the reservation and assignment of volumes. This service runs only if the server has devices under Media Manager control. The process is `ltid`.

NetBackup properties

Same as NetBackup configuration options but are called NetBackup properties on Microsoft Windows platforms.

NetBackup Request Manager service

The NetBackup Windows NT/2000 service that runs on the master server and starts the scheduler and receives requests from clients.

NetBackup Volume Manager service

A NetBackup Windows NT/2000 service that runs on a NetBackup server, allows remote administration of Media Manager, and manages volume information. The process is `vmd`.

NIS

Network information service.

NLM

NetWare loadable module.

NFS

Network file system.

nonrobotic

See "standalone."

ODL

Optical disk library. This robot type is supported only by NetBackup DataCenter servers.

OSF and Motif

A set of specifications for user-interface design.

outport

See "entry and exit ports."

partitions

The logical partitions into which a magnetic disk is divided.

patch

A program that corrects a problem or adds a feature to an existing release of software.

path length

Number of characters in a pathname.

pathname

The list of directories in the path to a destination directory or file.

PC clients

NetBackup clients that have Microsoft Windows (NT/2000, 98, 95), Macintosh, or IBM OS/2 operating systems.

peername

The name by which a computer identifies itself when establishing connections to other systems.

port

A location used for transferring data in or out of a computer.

primary copy

The copy of an image that NetBackup uses to satisfy restores. When NetBackup duplicates an image, the original is designated as the primary copy.

privileges

The tasks or functions that a user, system, or application is authorized to perform.

progress report

Log where NetBackup records events that occur during user operations.

proxy restore

A proxy restore allows the user to restore files, that he has write access to, on a machine other than his desktop. The files must be in a backup of the machine to which they are being restored.

QIC

Quarter-inch-cartridge tape.

queued job

A job that has been added to the list of jobs to be performed.

raw-partition backup

Bit-by-bit backup of a partition of a disk drive on UNIX. On Windows NT/2000, this is called a disk-image backup.

rbak

The program that Apollo clients use to read data from tape during a restore.

registry

A Microsoft Windows 2000, NT, 98, and 95 database that has configuration information about hardware and user accounts.

remote media server

A media server that is not the master. Note that only NetBackup DataCenter supports remote media servers. NetBackup BusinesServer supports only a single server, the master.

residence

In Media Manager, information about the location of each volume is stored in a volume database. This residence entry contains information, such as robot number, robot host, robot type, and media type.

resource

A Novell NetWare term that refers to a data set on the target. For example, in DOS, resources are drives, directories, and files. Also see "target service."

restore

(verb) The act of restoring selected files and directories from a previous backup or archive and returning them to their original directory locations (or to an alternate directory).

(noun) The process of restoring selected files and directories from a previous backup and returning them to their original directory locations (or to an alternate directory).

retention level

An index number that corresponds to a user-defined retention period. There are 10 levels from which to choose (0 though 9) and the retention period associated with each is configurable. Also see "retention period."

retention period

The length of time that NetBackup keeps backup and archive images. The retention period is specified on the schedule.

root

The highest level directory in a hierarchical directory structure. In MS-DOS, the root directory on a drive is designated by a backslash (for example, the root on drive C is C:\). On UNIX, the root directory is designated by a slash (/).

Also, a UNIX user name having administration capability.

RS-232

An industry-standard interface for serial communications and sometimes used for communicating with storage peripherals.

RSM Interface

Application in Windows 2000 used to manage Removable Storage Manager (RSM) devices.

RSM - Removable Storage Manager

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

Also, a component of the Windows 2000 operating system that manages storage devices.

RVSN

Recorded volume serial number. This is an identifier recorded as part of the label on a volume and used by Media Manager to ensure that the correct volume is mounted. The RVSN is the same as the media ID.

schedules

Controls when backups can occur in addition to other aspects of the backup, such as: the type of backup (full, incremental) and how long NetBackup retains the image.

SCSI

Small computer system interface. This is a type of parallel interface that is frequently used for communicating with storage peripherals.

slave server

See Remote media server.

server directed restore

Using the client interface on the master server to restore files to any client. Only the administrator can perform this operation.

server independent restore

Restoring files by using a NetBackup server other than the one that was used to write the backup. This feature is available only with NetBackup DataCenter.

server list

The list of servers that a NetBackup client or server refers to when establishing or verifying connections to NetBackup servers. On a Windows NT/2000 server and Microsoft Windows clients, you update the list through a dialog box in the interface. On a UNIX server and UNIX and Macintosh clients, the list is in the `bp.conf` file. On NetWare target and OS/2 clients, the list is in the `bp.ini` file.

service

A program on a Windows NT/2000 system that runs in the background and performs some task (for example, starting other programs when they are needed). Services are generally referred to as daemons on UNIX systems.

session

An instance of NetBackup checking its schedules for backups that are due, adding them to its worklist, and attempting to complete all jobs in the worklist. For user backups and archives, a session usually consists of a single backup or archive.

Shared Storage Option (SSO)

See "multihosted drives."

SMDR

Storage management data requestor, a Novell NetWare program that provides its services transparently to all SMS modules and lets remote and local modules communicate with one another.

SMS

Novell NetWare storage management services.

standalone

A qualifier used with drives and media to indicate they are not associated with a robot. For example, a standalone tape drive is one where you must manually find and insert tapes before using them. A standalone volume is one that is located in a standalone drive or is stored outside of a drive and designated as standalone in the volume configuration.

status code

A numerical code, usually accompanied by a message, that indicates the outcome of an operation.

storage migrator

Refers to the VERITAS Storage Migrator line of hierarchical storage management products for UNIX and Windows NT/2000. These products make extra room on a disk by transparently moving data to other storage and then transparently retrieving the data when it is needed by a user or application.

Storage Migrator is available only for NetBackup DataCenter servers.

storage unit

Refers to a storage device where NetBackup or Storage Migrator stores files. It can be a set of drives in a robot or consist of one or more single tape drives that connect to the same host.

SUSPENDED media state

If a volume is SUSPENDED, NetBackup can restore from it but cannot use it for backups. NetBackup retains a record of the Media ID until the last backup image on the volume expires.

symbolic link

On a UNIX system, this is a pointer to the name of the file that has the source data.

tape format

The format that an application uses to write data on a tape.

tape marks

A mark that is recorded between backup images on a tape.

tape overhead

The space required for data that is not part of the backup images. For example, tape marks and catalogs of what are on the tape are considered overhead.

tape spanning

Using more than one tape to store a single backup image.

tar

Tape ARchive program that NetBackup uses to extract backup images during a restore.

target

See “target service.”

target service

A Novell NetWare service that needs storage management. The SMS views all services (for example, print services, communication services, workstations) as targets.

Target Service Agent

A Target-service agent is a Novell NetWare agent that prepares the target's data for SMS during a backup and for the target during a restore.

TLD - Tape Library DLT

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

TLH - Tape Library Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

This robot type is supported only by NetBackup DataCenter servers.

TLM - Tape Library Multimedia

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

This robot type is supported only by NetBackup DataCenter servers.

TL4 - Tape Library 4MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

TL8 - Tape Library 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

timeout period

The period of time that an application has allotted for an event to occur.

TIR

See "true image restore."

tpconfig

A Media Manager administration utility for configuring devices and is started from the command line. On UNIX, it has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

transfer rate

The rate at which computer information is transferred between a source and a destination.

true image restore

Restores the contents of a directory to what it was at the time of any scheduled full or incremental backup. Previously deleted files are ignored.

TS8 - Tape Stacker 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

TSA

"Target Service Agent."

TSH - Tape Stacker Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web page at `www.support.veritas.com`. Choose NetBackup BusinesServer or NetBackup DataCenter in the VERITAS Support Product List and look under support options.

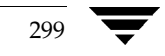
This robot type is supported only by NetBackup DataCenter servers.

user operation

A backup, archive, or restore that is started by a person on a client system.

verbose flag

Configuration file entry that causes a higher level of detail to be written in the logs.



verify

An operation that compares the list of files that are actually on a volume with what NetBackup has recorded as being on it. The data that is on the media is not verified.

vmadm

A Media Manager administrator utility for managing volumes. It runs on UNIX and has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

vm.conf

A Media Manager configuration file with entries that include the servers that can manage local devices and default media ID prefixes for media that do not contain barcodes.

volume

Media Manager volumes are logical units of data storage or cleaning capability on media that have been assigned media IDs and other attributes, which are recorded in the Media Manager volume database.

volume configuration

Refers to configuration information that is stored in the Media Manager volume database.

volume database

An internal database where Media Manager keeps information about volumes. All Media Manager hosts have a volume database. However, the database is empty unless the host is designated as a volume database host.

volume database host

The Media Manager host that contains information about the volumes that Media Manager uses in a device. Because NetBackup BusinesServer supports only a single server, the volume database host is always the Media Manager host.

volume group

A set of volumes that are configured within Media Manager to reside at the same physical location (for example, in a specific robot).

volume pool

A set of volumes that are configured within Media Manager to be used by a single application and are protected from access by other applications and users.

wakeup interval

The time interval at which NetBackup checks for backups that are due.

wbak

The program that Apollo clients use to write data on tape.

wildcard characters

A character that can be used to represent other characters in searches.

WORM media

Write-once, read-many media for optical disks. NetBackup BusinesServer does not support WORM media.

Windows Display Console

A NetBackup-Java interface program that runs on Windows 2000, NT, 98, and 95 computers. Users and administrators can start this interface on their local system, connect to a UNIX system that has the NetBackup-Java software installed, and then perform any user and administrator operations that their permissions allow.

xbp

The X Windows-based backup, archive, and restore program for users on NetBackup UNIX clients.

xbpadm

The X Windows-based NetBackup administration interface on UNIX. This interface is available only with NetBackup DataCenter.

xbpmon

The X Windows-based NetBackup utility for monitoring jobs on UNIX. This utility is available only with NetBackup DataCenter.

xdevadm

The X Windows-based Media Manager utility for managing devices on UNIX. This interface is available only with NetBackup DataCenter.

xvmadm

The X Windows-based Media Manager utility for managing media on UNIX. This interface is available only with NetBackup DataCenter.

Index

A

acssel, description 263
acsssi, description 263
acstest 275, 277
Activity logs 62, 74
admin log 63
admincmd, directory 244
Administration interface
  activity logging 74
  errors 72
All Log Entries report 61
Alternate client restores
  definition 280
  host.xlate file 273
Alternate path restore
  definition 280
Alternate target restore
  definition 280
altnames file 254
application server status codes (Java interface) 73
Archive bit
  definition 280
Archives
  definition 280
ascd, description 263
associate.bat file 75
Audience for manual ix
auto-configuration problems 15
avrd, description 263

B

Backup frequency
  definition 285
Backup images, definition 287
Backup process
  files 226
  Macintosh clients 233
  multiplexing 228
  NetBackup databases 234
  NetWare clients 232
  UNIX clients 226
  Windows 98/95 clients 230
  Windows NT/2000 clients 231
Backup Status report 61
Backup windows
  definition 281
Backups
  definition 280
bin
  Media Manager 262
  UNIX client 244
BP 241
bp
  description 245
  log 66
  UNIX client log 65
bp.conf file
  definition 281
  UNIX client/server 244
BP.NLM 245
bpadm
  description 245
bparchive
  description 245
  log 65, 66
bpbackup
  description 246
  log 65, 66
bpbkar
  description 246
  log 65, 66
BPBKAR32 231, 246
bpbrm
  description 246
  log 63
BPCD 232, 240, 241

bpcd
description 247
Mac client log 68
server log 63
UNIX client log 65, 67
BPCD.NLM 247
BPCDW32 230, 239
BPCDW32.EXE 247
bpclntcmd utility 35
bpdbjobs
description 247
log 63
bpdbm
description 248
log 63
bpdm
description 248
log 63
bperror command 77
bphdb
description 248
log 65
BPINETD 231, 240
bpinetd.log 66
bpjava-msvc 248, 249
bpjava-msvc activity log 74
bpjava-msvc log 63
bpjava-usvc activity log 74
bpjava-usvc log 63
bplist
description 249
log 65, 67
bpmount
log 65
bpmount log 67
bprd
description 249
log 63
bprestore
description 249
log 65, 67
bpsched
description 250
log 63
bpsrv
log 67
BPSRV.EXE 250
BPSYS.EXE 250
bptm
description 250
log 63

C

class database file 254
Client Backups report 61
Client user interface 282
Client, NetBackup
activity logs
Mac clients 68
UNIX clients 65
Windows and NetWare clients 66
configured name 271
installation problems 13
multiple hostnames 271
NT disk recovery 208
peername 271
software location
UNIX clients 244
testing configuration 18, 21
UNIX disk recovery 207
Clients, NetBackup
definition 282
Communications problems
PC clients 28
UNIX clients 24
config file 254
Configuration database 254
configuration device file does not exist 17
Configuration problems 13

D

Daemons
Media Manager 262
NetBackup 245
robotic 255
robotic control 255
Database directory, Media Manager 262
Database extension 223
Database recovery
identify media 212
procedure 214
Databases
Media Manager
device 262
volume 262
NetBackup
backup process 234
description 254
db directory, NetBackup 244

Debug level 67, 68, 74
Debug logs
NetBackup (see Activity logs)
vmd 69, 262
Define the problem 1
Device configuration problems 15
Device database 262
Directory structure
Media Manager 261
NetBackup
UNIX client/server 243
Disaster recovery 203
Disk recovery
media server 207
NT client 208
root on master 205
UNIX client 207
UNIX master server 203
Disk-image backup
definition 284
DLT, definition 284
DNS (see Domain Name Service)
Domain Name Service
hostnames 273
drive
drive limit exceeded 17
type not determined 18
driver directory 262
drives, too many 16
Duration to Keep Logs 63

E

Error codes (see Status codes)
Error database 254
Event viewer logging option 70
exception errors in Java Admin interface 72
exclude_list
UNIX client 244

F

failure_history file 254
File database 254
Files
archive process 226
backup process 226
host.xlate 273
restore process 236
format directory 262
Functional overview
introduction 223
Media Manager
device management 257
directories and files 261
programs and daemons 262
startup 255
volume management 257
NetBackup
backup and archive 226
directories and files 243
programs and daemons 245
restores 236
startup 224

G

goodies directory 262
goodies, directory 244

H

Help files
Media Manager 262
UNIX client 244
Host name entries, checking 32
host.xlate file 34, 273
HSM 287

I

IDR 208
Images database 254
Images on Media report 61
include_list
UNIX client 244
inetd, Mac client log 68
install_path 287
Installation problems 13
Intelligent Disaster Recovery (IDR) 208
Introduction to troubleshooting 1

J

Java interface
activity logging 74
troubleshooting background 72
jbpSA, overview 251
JBPSimple.properties file 74
Jobs database 254

L

Launch.properties file 74
Library, definition 288
license problems 16, 17
lmfs description 264
lmftest 275

Log level
Macintosh clients 68
Windows and NetWare clients 67
Logs
overview 59
activity, enabling detailed 74
activity, introduction 62
event viewer logging option 70
Mac client activity
bpcd 68
inetd 68
media management 69
NT Event Viewer Application 62
PC client activity
bp 66
bparchive 66
bpbackup 66
bpbkar 66
bpcd 67
bpinetd 66
bplist 67
bpmount 67
bprestore 67
bpsrv 67
nbwin 67
tar 67
user_ops 67
reports, NetBackup 61
server activity
admin 63
bpbrm 63
bpcd 63
bpdbjobs 63
bpdbm 63
bpdm 63
bprd 63
bpsched 63
bptm 63
xbpadm 63
xbpmon 63
system 62
UNIX client activity
bp 65
bparchive 65
bpbackup 65
bpbkar 65
bpcd 65
bphdb 65
bpjava-msvc 63
bpjava-usvc 63
bplist 65
bpmount 65
bprestore 65
obackup_tape 66
tar 66
user_ops 66
user progress 62
Logs directory
UNIX client/server 244
ltid, description 264

M

Master server, test procedure 18, 22
Media Contents report 61
Media database 254
Media host, definition 289
Media List report 61
Media Log Entries report 61
Media Manager
functional description 254
logs 69
Media Manager host
definition 290
Media server
definition 290
Media server, test procedure 21
Media Summary report 61
Media Written report 61
message
finding message text from status code 77
Messages, NetBackup 181
misc file 262
Motif interfaces 262
Multiplexed backups 228

N

NBNW95 232, 241
NBNW95.EXE 252
NBNWNT 232, 241
NBNWNT.EXE 251
NBWIN 230, 231, 239, 240
nbwin
log 67
NBWIN.EXE 251
NetBackup Administration interface
activity logging 74
errors 72
NetBackup Client service
definition 291

start and stop 12
NetBackup configuration options
definition 291
NetBackup Database Manager service
definition 291
start and stop 12
NetBackup Device Manager service
definition 291
start and stop 12
NetBackup Request Manager service
definition 292
start and stop 12
NetBackup Volume Manager service
definition 292
start and stop 12
NetBackupBPCD 233, 242, 252
NetBackupListen 233, 242, 252
NetWare Loadable Module 292
Network connections, multiple 271
Network problems
PC clients 28
UNIX clients 24
NLM (see NetWare Loadable Module)
Nonrobotic, definition 292
Novell
values affecting restore 89, 90

O

obackup_tape log 66
odld, description 264
odltest 276
Operating system errors 73
output, redirect to a file 75

P

pass-thru not supported 17
Preliminary troubleshooting procedure 9
Problems report 61
Procedures
recovery
media server disk 207
NetBackup databases 211
NT client disk 208
root on master 205
UNIX client disk 207
UNIX master server disk 203
troubleshooting
communications problems 24
host names and services 32
installation and configuration 13
introduction 9
master server and clients 18
media server and clients 21
preliminary 9
Processes (see Functional overview)
Programs
Media Manager 262
NetBackup 245
Progress logs, user 62

R

Raw partition backups
definition 293
Raw partitions
backup process 226
restore process 236
Recording information 2
Recovery procedures
importing media 212
NetBackup databases 211
NT client disk 208
root on master 205
server disk 207
UNIX client disk 207
UNIX master server disk 203
redirect output to a file 75
Related manuals x
Release notes, online copy 244
Remote media server
definition 294
Reports, NetBackup 61
Resource (also see Target service) 294
Restore process 236
NetWare client 241
Windows 98/95 client 239
Windows NT/2000 client 240
Restores
definition 294
Retention period
definition 294
robot
drive number unknown 17
robot limit exceeded 17
type not determined 16
unknown 16
Robot drive selection 257
Robotic control daemons 255
Robotic daemons 255
Robotic test utility 275

acstest 275, 277
odltest 276
RSM robot 277
tl4test 276, 277
tl8test 276, 277
tldtest 276, 277
tlhtest 277
ts8test 276, 277
tsdtest 276, 277
tshtest 276
Robotic test utilitylmftest 275
robtest 275, 277
root 294
RSM robot 277
rsmd, description 265

S

Scheduler, bpsched 63
serialization problems 15
Server
disk recovery 207
installation problems 13
NetBackup activity logs 62
recovering root on master 205
test procedure for master 18, 22
test procedure for media server 21
UNIX disk recovery 203
Server directed restore
definition 295
Services entries, checking 32
Session, NetBackup 296
slots, too many 16
SMS (see Storage Management Services)
Software version, determining
Macintosh clients 88
Media Manager 262
NetWare nontarget clients 88
NetWare target clients 88
UNIX client/server 244
UNIX servers 87
Windows clients 88
Windows NT servers 88
Standalone
definition 296
Startup
Media Manager process 255
NetBackup 224
status code
finding message from 77
Status codes, NetBackup
sorted by code 77
sorted by message 181
stderr 72
stdout 72
Storage Management Services 296
Storage Migrator 297
Storage units
definition 297
syslogd 62, 69
System logs 62

T

tar
log 67
tar, NetBackup 252, 253
TAR32 240
Target Service 298
Test utility, robotic 275
tl4d, description 265
tl4test 276, 277
tl8cd, description 266
tl8d, description 265
tl8test 276, 277
tldd, description 266
tldtest 276, 277
tlhcd, description 267
tlhd, description 267
tlhtest 277
tlldcd, description 266
tlmd, description 267
tpconfig, definition 299
tpconfig, overview 268
traceroute 273
Troubleshooting procedure
communication problems
PC clients 28
UNIX clients 24
general
introduction 18
master server and clients 18, 22
media server and clients 21
host name and services entries 32
installation 13
preliminary 9
True image restore
definition 299
ts8d, description 269
ts8test 276, 277

tsdd, description 268
tsdtest 276, 277
tshd, description 268
tshtest 276

U

user_ops log 63
Utility, robotic test 275

V

Verbose option 64
VERITAS NetBackup ix
Version, software (see Software version, determining)
vm.conf file 262
  definition 300
vmadm, definition 300
vmadm, overview 269
vmd
  debug logging 69
  overview 269
Volume database 262
Volume database host
  definition 300
Volume database, definition 300
Volume group
  definition 300
Volume pool
  definition 300

W

Windows Display Console 75
WORM media
  definition 301

X

xbp, overview 253
xbpadm log 63
xbpadm, overview 253
xbpmon 253
xbpmon log 63
xdevadm 262
xdevadm, overview 269
xvmadm 262
xvmadm, overview 270